AN INVESTIGATION OF ONLINE THREAT AWARENESS AND BEHAVIOUR PATTERNS AMONGST SECONDARY SCHOOL LEARNERS

A thesis submitted in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

Of

RHODES UNIVERSITY

MICHAEL PADRIC IRWIN

December 2012

ABSTRACT

The research area of this work is online threat awareness within an information security context. The research was carried out on secondary school learners at boarding schools in Grahamstown. The participating learners were in Grades 8 to 12.

The goals of the research included determining the actual levels of awareness, the difference between these and self-perceived levels of the participants, the assessment of risk in terms of online behaviour, and the determination of any gender differences in the answers provided by the respondents.

A review of relevant literature and similar studies was carried out, and data was collected from the participating schools via an online questionnaire. This data was analysed and discussed within the frameworks of awareness of threats, online privacy social media, sexting, cyberbullying and password habits. The concepts of information security and online privacy are present throughout these discussion chapters, providing the themes for linking the discussion points together.

The results of this research show that the respondents have a high level of risk. This is due to the gaps identified in actual awareness and perception, as well as the exhibition of online behaviour patterns that are considered high risk. A strong need for the construction and adoption of threat awareness programmes by these and other schools is identified, as are areas of particular need for inclusion in such programmes.

Some gender differences are present, but not to the extent that, there is as significant difference between male and female respondents in terms of overall awareness, knowledge and behaviour.

ACKNOWLEDGEMENTS

I would like to acknowledge the support and encouragement of my family throughout the process of writing this thesis. Thanks too must go to my Supervisors. Karen Bradshaw for her patience, attention to detail, sound advice, and determination to help me get things done correctly, all of which is greatly appreciated; and Ingrid Siebörger for her fresh perspective and valuable advice, especially regarding terminology and engagement with schools. Last, but by no means least, I would also like to thank Joe Alfers in particular, whose support and co-operation, as my manager, over the past two years has been exceptional.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The aim of this chapter is to provide an introduction to the specific research into information security threat awareness. The area of research itself is discussed, followed by an explicit statement of the problem being investigated, the relevance of the specific topic, the scope of the project, as well as the goals of the research. This section also clearly states what was not covered (for reasons of scope or logistics or purely for clarification) in this research.

1.1 RESEARCH AREA

The general area of research is information security, and within that, threat awareness. More specifically, the research relates to the awareness of information security risks amongst young adults. The purpose of the research is to gain insight into both current levels of awareness amongst the selected target group of senior (Grades 10-12) secondary school Learners (see Section 1.3), as well as the online behaviour patterns and experiences of the respondents. This assessment is done via an online questionnaire. Part of the analysis of the research is to determine if there are any significant differences between genders in terms of awareness and relevant online behaviour related to information security. Online privacy forms part of the general area of threat awareness and this is a recurring theme in the questionnaire through which the data was collected.

1.2 SCOPE OF THE RESEARCH

The target group of the research is secondary school learners, in the 16-18 year age group who have regular access to computers, cellular telephones, and the Internet. The schools utilised for research are in the Grahamstown area. As these schools offer boarding facilities, it is highly likely that there would be a significant variation in the background, race, gender, socio-economic status and home location of the learners. This was considered desirable in order to provide the research with a wider range in terms of responses than if the target group were fully homogenous. It could thus provide value in terms of applicability across a broad spectrum of schools.

The scope of the project includes the areas of threat awareness relating to information security, online behaviour, and online privacy, as they are all inter-related. Areas of focus on the practice of sexting and on cyberbullying are included. With the scope limited by the time and size constraints of the research project, no models were developed, but the information gathered during the research provides a basis for future research into the relevant aspects thereof. No actual training or formal implementation or development of threat awareness programmes took place..

1.3 RESEARCH OBJECTIVES

The objectives of the research are to produce data that can provide insight into the awareness of information security threats and online behaviour at secondary school level, within the declared age range, and within context of information security. Data is required across the following focus areas: types of threats, risks posed by these threats, actual online behaviour, online privacy, cyberbullying, actual experiences and perceptions. Sub goals of the research include investigating gender differences and the correlation (if any) between perceived awareness and actual knowledge (awareness), as well as behaviour, based on answers given directly for both awareness and online behaviour. Henceforth in this thesis, reference to 'actual behaviour' is based on the respondents' answers to relevant survey questions.

The statement of the research problem is: to confirm the hypothesis that secondary school learners aged 16 to 18 have limited knowledge of information security threats facing them through the use of the Internet and cellular telephones.

1.4 RELEVANCE OF THE STUDY

A common estimation is that as many as 65% of computer users (Skinner 2010) have knowingly or not been a victim of cybercrime. This figure, even if partially accurate, provides ample reason for the notion of threat awareness to be taken seriously.

Threat awareness is a relevant topic of research in information security, in terms of determining what existing and potential or developing threats are, and being aware of how they can be mitigated. One of the methods of mitigating threats is to make the

people who are open to compromise or who use systems that could be compromised aware of the threats and how to avoid them.

Successful implementation and conveyance to people of the importance of the awareness of information security threats has the potential to significantly reduce the impact of cybercrime, online vulnerability, malware in general, and other threats. In terms of threat awareness in practice, the corporate world is the major employer of awareness strategies and training or education programmes. This is due to the fact that a compromise of organisational security can result in the compromise of corporate data, loss of competitive advantage, or catastrophic data loss. All of these result in financial impairment. While the latter is not the major potential loss in a school environment, other consequences abound, including but not limited to, harm to the reputation of the school, mental and physical harm to those within the school environment, as well as the more common loss of control over information, and data loss.

There are some examples of threat awareness programmes at universities although personal research has indicated that these are present primarily in America. Even there, universities with such programmes are in the minority. To date no such programme has been identified at a South African university. Speculatively, this may be because corporates are more obvious targets, and have more to lose by being targeted than a university. It may also be that as a result of thinking such as this, universities do not regard themselves as either being targets or having the potential for significant loss or damage to function caused by information security breaches. Where the next largest gap in threat awareness programmes appears is at the next level down, at secondary school level. Research done on awareness at this level is almost non-existent, and the implementation of programmes even less so. This alone puts the research area, and indeed the completed research itself into stark relevance.

While threat awareness is important at all times, this is especially so at this secondary school stage. This is because early exposure to sound subject awareness can translate into better safer online behaviour and use of technology in the workplace, and home throughout the user's life. This in turn has the potential to reduce future compromise of the individuals and the institutions of which they are part.

1.5 ASSUMPTIONS UNDERPINNING THE RESEARCH

Prior to the commencement of the research, a number of assumptions were made about what the research might reveal in terms of awareness levels and behaviour patterns. These assumptions are that the respondents would rank their usage of social media platforms as high, that cyberbullying, while not expected to be widespread, would still appear as statistically relevant in terms of victim and participant numbers, and that the respondents would derive value from the exercise of answering the questionnaire, not in terms of raising their actual awareness in terms of in depth knowledge, but in terms of becoming more aware of threats generally. As is evident from the discussion of the results, some of these assumptions were correct, and others less so. Nonetheless it was these assumptions, alongside the desire to investigate their veracity, which lead to the formulation of the research goals outlined above.

1.6 THESIS STRUCTURE

The remainder of this thesis is structured as follows: Chapter 2 explores the concept of threat awareness and related research. Following this, Chapter 3 covers elements of the research design and data gathering process, pre-research assumptions and the methodology used. The analysis and discussion of results follow, in Chapters 4 to 7. Chapter 4 covers the awareness of threats based primarily on terminology, while Chapter 5 explores the concept of online privacy and its relevance to social media. Chapter 6 tackles the behavioural issues of sexting and cyberbullying. Password habits are investigated in Chapter 7, before the final conclusions and information regarding potential avenues for future research based on the finding of this project are presented in Chapter 8.

CHAPTER 2: LITERATURE SURVEY

The research topic is not one that has been extensively studied, and so there is a comparative lack of academic literature available in the form of books and peer reviewed studies or journal articles. There are however some studies that have been conducted, which include elements similar to or relevant to the proposed topic. These are highlighted in this chapter, along with some theoretical material on the area of research to provide context to the study. While the construction of an awareness programme did not form part of the research, factors that could lead to the construction of such a programme, are identified through the results obtained. Some principles and concepts relevant to such a programme, are included, on the basis of their being part of the broader research area of awareness of threats. A further purpose of this survey is to broadly introduce the elements of (online) threat awareness, and to provide some information regarding some of the terminology used.

2.1 PRINCIPLES OF THREAT AWARENESS

While the construction of an awareness programme and user education falls beyond the scope of this research (as stated above), it is relevant to bear in mind principles of success in dealing with awareness of information security threats in the corporate world. This information could assist in the development of the research questionnaire. Evaluation of risks and threats is a foundation principal of, and was carried out as, the goal of the research upon which this thesis is based. Vacca (2009:7) suggested commencing the process of securing an organisation by evaluating potential threats to it. This was the goal, and outcome of the research undertaken, albeit in the context of school learners, rather than in a corporation. Potential threats were assessed on the basis of awareness and practice as exhibited by school learners as respondents to an online questionnaire.

Vacca (2009:7) further stated that "Perhaps the most common misconception is that the [particular] business is obscure, unsophisticated, or boring – simply not a target for malicious activity." This may be the reason for the current lack of awareness programmes in schools generally, which is a statement based on research into the existence of such programmes. It may be true that schools as a type of organisation are

less tempting targets for information thieves than other organisations. Nonetheless the individual learners in the schools remain potential targets for information theft, albeit in some different ways, and for different reasons to corporations and corporate employees. While the consequences for information breaches amongst school learners and corporates would be considered different in terms of broad impact and scale, the impact on individuals, especially the young, can be no less important, and potentially very harmful.

Taking the above into account the research focused on the respondents both as individuals and as a group, rather than on the schools as organisations. This people-oriented as opposed to organisational emphasis is present throughout the research. It is clear though that the results obtained could be used subsequently to assist with aspects of organisational security enhancement, in this case, through one element of the security makeup of the school as an organisation: the learners.

Another principle adhered to in this research is thinking outside the box. This process refers specifically to paying heed to threats within the organisation, rather than external threats (Vacca 2009). In a school sense this relates to the personal consequences for learners involved in information compromise or compromising behaviour amongst their peers. An example of this would be to consider that cyberbullying could take place from within the school, and is perhaps more likely to do so, than to originate from an external source.

Parker (2002) listed the principles of providing security training to Information Technology (I.T.) staff, and the development of a security culture amongst employees. Parker (2002) was of the opinion that "Training people to be careful and holding them accountable for protecting information, may be the most effective means of preventing endangerment." The principle of accountability is one which is conceivably more applicable to corporate employees than school learners. If personal accountability and a sense of personal responsibility for action, and their consequences could be encouraged from a young age it would remain an effective principal throughout their individual lives.

Similarly, Vacca (2009:12) stated that "One of the greatest security assets is a business's own employees, but only if they have been trained properly to comply with security

policies and potential problems." In a school environment this would refer to the prevention of incidents that may reflect poorly on the school as a whole, and the resultant consequences of such incidents. Prevention of such incidents could be achieved through the implementation of relevant awareness programmes and education. The notion of personal behaviour impacting on the school as a whole was not directly addressed during the research, but by implication it certainly helps to emphasise the importance and relevance of the research in terms of potential impact and consequence.

Related to this impact, as mentioned by Vacca (2009), is the fact that security problems with regard to employees can and do include that employees either do not understand the significance of adhering to security procedures, or worse, view them as an inconvenience. Both of these issues could be addressed by education. If one substitutes learners for employees, this statement could hold true within a school environment. Indeed, as is apparent from the discussion on privacy in Chapter 5, there is evidence of misunderstanding, and potentially negligence on the part of the learners. While it was not specifically determined, this could have been based on viewing adherence as an 'inconvenience' as suggested above. The focus of the research thus remained on determining information relevant to the learners themselves, so that significance and inconvenience could potentially be dismissed as barriers to valuing awareness and safe online behaviour.

Considering the research area, that is, threat awareness in an information security context, Mitnick and Simon (2005:240) state that "…the best motivating factor may be that no-one likes to be manipulated, deceived, or conned. As such, people are highly motivated to not feel foolish or stupid by falling for some scam". While this is certainly a relevant approach to take when implementing an awareness programme, or providing any form of user education to companies or institutions where information security is paramount, it is also potentially relevant to the school environment, and thus to the results obtained throughout this research.

While the sentiments expressed by Mitnick and Simon (2005) above regarding manipulation and deception were taken into account, the research emphasis remained on *awareness* and the need for education in terms of identifying the general and area

specific needs for it amongst the group of respondents surveyed, rather than the construction of an educational programme. In spite of this, the exposure to terminology and other questions during the course of the survey may have provided cause for the respondents to become more aware of threats, and therefore less likely to want to fall victim (Mitnick and Simon: 2005).

van Niekerk and von Solms (2008) applied Bloom's Taxonomy to information security education. This taxonomy (or classification) is a hierarchical classification of forms and levels of learning, within an educational context (Atherton 2011). While this paper by van Niekerk and von Solms (2008) did not target schools specifically, as this research does, it provided insight into the importance of user education, which is a natural follow-on or outcome from the stated research goals (see Section 8.2).

A problem raised by Van Niekerk and von Solms (2008:1) is that "Most current information security education programmes are constructed by information security specialists who do not necessarily have a strong educational background." As such, their research investigates the *educational needs* of people, which is what is covered in this research: the identification of a need for education and the specific areas requiring it. The conclusion drawn from their paper is that "…the common categorization of security educational needs into the broad categories of awareness, training, and education, is not ideal…" (in an educational context). Instead it is suggested that these areas be assessed, and defined though the use of an educational taxonomy, based on educational rather than purely security based needs. Needs assessment forms the basis for the questionnaire administered to respondents, and thus too the basis of this research.

Continuing with a focus on educational needs, Roper, Fisher and Grau (2005) were of the opinion that awareness education is often carried out without investigation into, and understanding of, the factors that need to be addressed. Their research addressed this problem through the investigation and understanding of the factors which lead to the need for threat awareness among a group of respondents, which thus could in turn have broader implications for the construction and implementation of relevant educational / awareness programmes to address the areas of concern identified in this research, based on the answers obtained from the questionnaire completed by school learners.

Johnston and Warkentin (2010) conducted a study which included the use of surveys, on the effectiveness of the use of fear appeals on end users. More specifically, their goal was to determine whether fear appeals were an effective means of ensuring end user compliance with instructions regarding mitigation of threats. Included in their research was an element of awareness education. The target group in their research was a mixture of staff and students from different faculties and departments of a single university. The result of their research was that fear appeals are an effective tool in ensuring compliance regarding mitigation of threats.

In contrast, Boyd and Hargittai (2010) indicated that fear is a "less than ideal" approach, and outlined reasons why this is so, focussing primarily on the potential long term effects of fear in terms of restricting exploration of technology. In terms of the questions posed to the respondents, the effectiveness or otherwise of the use of fear (of the consequences of lack of awareness and risky online behaviour) was not evaluated. Moreover, based partly on the view expressed by Boyd and Hargittai above, no attempt was made during the composition of the questionnaire to include articles or questions that were intended to invoke fear amongst the respondents. Another reason for the exclusion of fear as an approach was that the questionnaire sought to investigate the respondents' answers as they were, rather than potentially compromise answers by 'scaring' respondents into providing answers they may not otherwise have given.

2.2 DEFINITION OF TERMS

Several technical terms are used in this thesis and in the questionnaire, specifically in the questions determining the respondents' awareness of these terms as online threats. While some of these could be considered self-explanatory to an extent, others require further clarification. Additionally, the terms used as the headings for each of the chapters are explained. The terms introduced as measures of actual threat awareness in the questionnaire, with the exception of *computer worms*, and *computer viruses* (due to their ubiquity in the public domain) are introduced and discussed.

Phishing is a term that has enjoyed increasingly popular usage, particularly as a result of the increase in 'phishing scams' encountered by the ordinary computer user. At its most basic, phishing can be defined as "…stealing identity information from users online…"

(Lininger and Vines 2005:xxi). Harley (2006:48) states that "in its most usual current form it masquerades as a communication from a banking establishment asking the recipient to re-enter their banking details into a form that appears to be generated at a legitimate banking site." Phishing does take other forms too, as implied, for example, emails purporting to be from email service providers requiring the user to input credentials on the pretext of enhancing their security, or any of many other reasons intended to lure the recipient into compliance.

Similarly, phishing emails could come from web-based social media platforms such as *Facebook*, making similar requests to the recipients. This kind of action would pose a direct threat to the participants in this survey, perhaps more so than the aforementioned fraudulent banking scams. However with the rise of online banking, even amongst the youth, this should not be discounted as a potential threat. Aside from being used to commit financial fraud, phishing is also a tool through the use of fake or 'spoofed' web pages with a legitimate look which can be used to acquire other personal information, such as date of birth, national identity numbers, and bank account numbers, all of which can be used in identity theft (Harley 2006) by taking advantage of a user's naivety. This makes it a dangerous threat to the unaware, and very relevant to the respondents, and is an example of where awareness can greatly reduce potential compromise.

Identity theft, most simply, is the theft of someone else's personal information and the use thereof in order to impersonate that person, primarily for financial gain. It is defined by Lininger and Vines (2005:268) as "…a crime in which an imposter obtains key pieces of personal information … in order to impersonate someone else". (Lininger and Vines 2005) stated further in 2005 that at the time identity theft was one of the fastest growing crimes. As noted above, there is a strong link between identity theft and phishing, with the latter carried out to allow the execution of the former. Although the two activities are related, they are by no means inseparable. There are other methods besides phishing of stealing or gaining access to personal information, such as card skimming (the copying of bank card details) or 'dumpster diving' (searching through rubbish bins for information). In terms of online threats, phishing is the primary method.

What the two terms have in common is that traditional defences for home users, and even corporate users, such as anti-virus software and firewalls are unable to defend the user. The only method of defence is through awareness and education: what to click on and what not to click on, where to enter one's user credentials, where not to, and how to spot the differences between legitimate and illegitimate emails and websites. Both phishing and identity theft have links to social engineering, forming the methods, and goals, respectively of some social engineering attacks.

Related to phishing, are *vishing* and smishing. The former, according to Jakobsson and Ramzan (2008) is 'voice-phishing', or phishing by voice rather than through web or email based methods as mentioned previously. Maggi (2010:1) defines vishing as "…the activity of systematically defrauding account holders using social engineering over the telephone system." Vishing is noted by Griffin and Rackley (2008) as having much potential as a very successful method identity theft and /or fraud. Typically vishing takes place either by the victim receiving a call and getting an automated message purporting to be from a known institution instructing them to enter personal information such as banking details, or being directed to call a number via an email. The latter would, for example, inform this person that their account has been compromised and that they need to call the number provided in order to verify their details as per Ollman (2007). Vishing is usually done over landline telephones, making use of Voice-Over-IP, and as such perhaps poses less of a threat to the respondents of this survey than phishing, although there are occasions when live rather than recorded calls form part of a vishing attack (Maggi 2010).

Taking into consideration the potential prevalence of mobile phone use amongst the group of respondents to this survey, *smishing* could be regarded as a greater threat than vishing according to the demographic of the respondents. The term is a combination of SMS (Short Message Service) and phishing. Siciliano (2012) defines smishing thus: "…smishing is a version of phishing in which scammers send text messages rather than emails, which appear to have been sent by a legitimate, trusted organization and request that the recipient click on a link or provide credentials in a text message reply". It is worth noting that vishing, smishing, and phishing can be linked to form combination, or hybrid attacks, and that all are techniques for electronic social engineering attacks.

Social engineering is a term used throughout this thesis, and several definitions are used in the discussion. Each one provides a slightly different insight into the term and is used in discussion as appropriate to the specific material under discussion. Mitnick and Simon (2002:*xi*) define *social engineering* as "…getting people to do things they wouldn't ordinarily do for a stranger." Mann (2008:11) expanded this definition as "to manipulate people, by deception, into giving out information, or performing an action." Hadnagy (2010: 10) in turn stated that "…a true definition of *social engineering* is the act of manipulating a person to take an action that may or may not be in the 'target's' best interest. This may include obtaining information, gaining access, or getting the target to take certain action." All three authors quoted provided relevant information on the topic of social engineering. The works of these authors have particular relevance to Chapters 5 and 6.

The *419 scam*, so called because of the section of the Nigerian penal code that the practice violates, (Lininger and Vines 2005), could also be regarded as social engineering, albeit in an unsophisticated form. It is defined in the Longman's Dictionary of Contemporary English as "an illegal way of getting money from someone by sending them an email promising that they will make a lot of money if they invest in a business activity which does not really exist"(Longmans Dictionary 2012). Essentially the purpose of the scam is to entice the recipient of the email or text message into paying an advance fee, in the hope of securing further wealth for the enticer, based on the premise laid out in the scam communication. The respondents' reactions to unsolicited, impersonal communications are assessed and discussed in Chapter 4. Whilst 419 scams could be considered a crude form of social engineering, they also fall into the category of spam.

Spam is defined by Harley (2006) as being unsolicited bulk email, which may or may not be commercial in nature. As with the 419 scam, it can also have criminal rather than advertising based intent. Harley (2006) notes too that there is a correlation between viruses, trojans, and spam, with spam being a delivery method for viruses and trojans. This serves to illustrate how many facets of, and terms relating to, information security are interwoven. Lininger and Vines (2005) state that up to two thirds of email globally, could be considered spam. This number illustrates the importance of education dealing with spam, beyond the annoyance factor, as the majority of users, including those

matching the characteristics of the respondents to this survey, would encounter spam in its various forms, including via text messages to their cellular telephones. This reveals another overlap in both threat and terminology, this time with smishing and social engineering.

Browser poisoning, sometimes called *search engine poisoning*, refers to "…the process of tricking the search engines into ranking an SEO (Search Engine Optimisation) page high up in the search results. Those results can be regarded as poisoned" (Howard and Komili 2010:2). The way in which the search engines are 'poisoned', is via scripts that create web pages loaded with key or topical terms which would result in a high hit count when any of those terms were searched for using a search engine. In this way the page is rated higher by the search engine, and so appears further up the search results list produced by the search engine (Howard and Komili 2010).

This in turn results in more clicks or 'hits' on the website, which is how users become infected with *malware*: through clicking on the link to the site itself. Howard and Komili (2010) recommend the best forms of defence to be examination of content combined with URL filtering. While this may be beyond the interest and skill level of the average user, information about the existence of such threats may be useful in terms of introducing people to some of the more complicated threats to their online safety and security.

Spoofing, loosely defined by Lininger and Vines (2005:8) as "…to pretend to be something you are not", has different potential manifestations. This is concurrent with the succinct definition provided by Braynov (2006:68) that spoofing is "a variety of techniques used to assume a false identity." These can include emails purporting to be from one sender but in actuality are from another, and IP addresses which are made to appear as if they belong in or originate from within a certain network, when in fact they do not. Tipton and Krause (2004:3201) summarise spoofing as "…the deliberate inducement of a user or resource to take incorrect action." This generally refers to the employment of electronic means to carry out this inducement. The action of spoofing has relevance to other terms covered, including 419 scams, social engineering, phishing, smishing, and vishing.

Some of the terms used in the testing of respondents' recognition of threat terms fall under the umbrella of *malware*. These related terms include crimeware, spyware, keystroke logging, and trojans. Malware itself is broadly defined by Vacca (2009:7) as "…software designed to infiltrate or damage a computer system without the owner's informed consent." This definition is broadly applicable to the related terms mentioned as falling under the category of malware in the previous sentence.

Crimeware is loosely defined by Jakobsson and Ramzan (2008:11) as follows: "…with more and more people conducting transactions online, malicious code moved away from being simply malicious and moved towards being criminal. This trend has given rise to a new form of malicious software – namely, *crimeware*." This term is also defined by Bernard (2005) as malicious software designed primarily to assist in the theft of identification information for use in financial crime. An example of a *crimeware* related cyber-attack, is the National Infrastructure Protection Centre (in the United States of America) advisory issued regarding the extortion of e-commerce and e-banking sites by 'Eastern European computer criminals, as described by Campbell and Kennedy (2002). In this example, the criminals managed to compromise approximately one million credit cards, successfully targeting some 40 companies. When this statistic is coupled with the more recent figure provided in the 2010 Norton Cybercrime Report (Norton 2010) that organised crime accounts for up to 90% of cyber-attacks, then the relevance of crimeware as a threat term becomes apparent.

A very sophisticated, and successful, example of crimeware is the *Conficker* worm. This worm was released in 2008, and managed to infect approximately half a million computers globally in the first month after its release (Bowden 2010). The first function of the worm was to infect machines and thus put them at the disposal of the creators, for use as a *botnet* (a group of security-compromised computers under the remote control of a third party).Thereafter, with *Conficker,* nothing major ever happened in terms of payload but the potential existed for large scale PC-based global mayhem. Regarding this Bowden (2010) emphasises the value of botnets to criminal endeavours due to their potential use for large scale malware distribution, information theft and denial-of-service attacks (flooding a computer or computers with response requests exceeding its ability to respond), amongst other uses. Bowden (2010) also notes the

commercial value of botnets: they can be sold by and to criminals for the uses already described.

How vulnerable the respondents in this survey would be to crimeware is largely dependent on their use of Internet banking and ownership of or access to credit cards, which was undetermined. Crimeware falls into the broad category of relevant online threats, taking into account that the respondents, some of whom were in their final year at school, could potentially be further exposed once outside of the school environment both upon exiting the school system, and while at home during school vacations. During these periods they would fall outside of any protection afforded them by the school.

Spyware is defined by Lininger and Vines (2005:106) as "…any technology that aids in gathering information about a person or organisation without that person's knowledge or consent…", a definition concurred with by Chan (2006:136), who also notes that "Spyware applications are typically bundled as a hidden component of freeware or shareware programmes that can be downloaded from the Internet." The purposes of spyware, as described by Lininger and Vines (2005:107) include the tracking of personal movement on the Internet for advertising and marketing purposes, criminal purposes as in the case of identity theft, as well as government or corporate monitoring. Since spyware is covert in installation, and not detected by anti-virus software (Chan 2006), it poses a threat to most web users, particularly those who download software or other items, such as games, video or music files from the Internet.

Keystroke logging programmes serve as an example of spyware, although also fit under the broader umbrella of malware, and even crimeware. Lininger and Vines (2005:108) define keystroke loggers as "…a form of spyware that records user keystrokes…they record every key typed on a computer, sending this information to the person who installed it …" Keystroke loggers can be installed via software (as part of an inadvertent spyware download for example), or can be physically connected to a machine in the hardware configuration, disguised as a USB stick for example. In either event, the potential for sensitive data loss is significant, with passwords, banking credentials, personal correspondence and account information all at risk. This potential for data compromise, along with the unobtrusive and automated installation method makes keystroke loggers a relevant threat, especially those prone to downloading files from

the Internet. Given the difficulty of detecting *keystroke loggers*, (as is the case with some other forms of spyware and crimeware) the threat posed is significant.

Similar to spyware in the sense that they are covert in their installation, are *trojans*, which are distinct from *viruses* and *worms*, and can be defined as programmes which "… masquerade as a legitimate, useful program, while performing malicious functions in the background." (Vacca (2010:124). Like spyware, users are vulnerable through their own actions in downloading the malicious software, providing another situation where awareness and education could assist with prevention. Unlike spyware, trojans not only have an information theft function, but also contain features that can allow an attacker remote access to the system onto which the trojan has been installed. Young (2006) notes that there are several different methods of attack using trojans, and that the point of a trojan is not to be noticed by the user of the machine on which it is installed, while carrying out its designated tasks. These methods include the termination of security related tasks and programmes, including anti-virus software.

The Oxford Dictionary definition of the term *sexting*, which is the one used as the benchmark for the purposes of this research is "…the sending of sexually explicit photographs or messages via mobile phone" (Oxford Dictionary 2012). The definition provided above is expanded for the purposes of this research to include the transmission of such material by electronic media other than mobile phone including email, instant messaging and social media platforms. Sexting is directly related to information security in terms of information disclosure of a personal nature and the consequences thereof, and especially online privacy.

Relevant to the discussion of sexting, are the South Africa Sexual Offences and Related Matters Amendment Act 32 (2007), and the Child Justice Act 75 (2008), which provided the legal consequences of engaging in activities that are by definition included in the action of sexting.

Belsey (2012) defined the term *cyberbullying* thus: "Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others."

The concept of *online privacy* features as a thread that runs throughout the research and discussion. Ianella (2006:877) defined privacy simply as "the act of ensuring personal

information is kept secret." Westin's definition of privacy as a concept as cited in Marwick, Murgia-Diaz and Palfrey (2010), is the "…claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Naturally, this translates to the online environment where the risks to keeping personal information secret and available only to those whom one would choose to make it available to, come both from external threats such as those previously defined, and from personal behaviour online. The latter in particular are addressed in some detail in this thesis.

Social media is also an area that features strongly in this research, owing to its status as a portal for privacy breaches and cyberbullying. "Children need to know that future employers and friends can follow their digital footprint online, something that could negatively affect their professional and private lives" (Donath 2010). This idea is addressed in both the questionnaire and subsequently in the discussion in this thesis,, with emphasis on the involvement in and consequences of sexting, and in terms of privacy concerns and the potential for cyberbullying by peers.

The reader is referred to online repositories such as http://www.athinline.org/ (Unknown A 2011) and http://www.cybertrapsfortheyoung.com (Lane 2011) for information and safety tips regarding privacy, sexting and cyberbullying. Information resources such as press articles on real incidents of cyberbullying, and anecdotes provided by these websites and others, including some of the news sources are referred to in the research via Appendix A in the context of providing illustrative examples.

2.3 SIMILAR STUDIES AND RELATED MATERIAL

The focus of this section is on studies that have been carried out by others, and which bear some similarity to the aims of this thesis in terms of subject material and/or the ages of respondents.

Notably in South Africa, there is a "…lack of structure or guidance for schools on how to deal with cyber threats. There are no clear procedures that are consistently followed by schools, governing boards and educators, and the cyber threat process is not widely known and understood by educators, learners …" (Sonhera, Kritzinger, Loock 2012). This further emphasises the need for such education, and especially so in South Africa.

This in turn enhances the relevance of this research, which although not providing procedures and programmes, does establish both the need, and areas for targeting in programmes such as these.

Of direct relevance to social media and privacy, and *Facebook* in particular, and more broadly applicable across the research area is the work by Boyd and Hargittai (2010) Of particular interest is the conclusion reached that their data indicated that the majority of their research subjects (young adults) were to some degree actively engaged with the privacy settings available to them. As similar issues are addressed in this thesis, this work has some value in terms of comparison with the results of the research carried out in this thesis (see Chapter 5). This survey by Boyd and Hargittai (2010) was carried out with students in higher education as the survey respondents, with many only a year out of school. As such while the age range of respondents was not exactly the same as those used in this thesis, the results are still broadly comparable. *Facebook* as a social media platform was focussed on in the discussion of the results obtained, adding to the relevance of this paper across other social media platforms and other information security threats, specifically online privacy in a broader sense.

In contrast Debatin, Lovejoy, Horn and Hughes (2009) reported in their study on *Facebook* and privacy that "Risks to privacy invasion were ascribed more to others than to the self. However, users reporting privacy invasion were more likely to change privacy settings than those merely hearing about others' privacy invasions." This finding points towards a lack of awareness, a lack of perceived need or desire to take action to improve privacy, or a combination of these factors.

Steeves (2010) carried out a survey of existing studies on online youth privacy. This summarises other research carried out relating to 'youth privacy'. The age range was more expansive than in this thesis, with younger respondents included, but comparison with the results produced is still possible. Worth noting is Steeves' (2010) research indicating that "…safety oriented campaigns are ineffective because they focus on dangers that are both highly unlikely and at odds with young people's social experiences." Bearing in mind that this statement referred specifically to privacy issues and not the broader range of information security threats, it remains relevant to this research not in terms of the construction of an awareness or education programme, but

in terms of the stated goal of this research; that is, to identify the actual areas of security weakness in the respondents' knowledge *and* their online behaviour and social experiences. The findings of this study, which investigated the actual experiences of respondents, could be considered relevant to future educational initiatives intended to address issues of *online safety* or awareness, particularly as it investigated the *actual* experiences of the respondents, potentially therefore negating the problem mentioned by Steeves above. This research into privacy by Steeves (2010) also provided evidence of gender differences in both attitudes to online privacy and behaviour, with girls shown to be more concerned and more proactive about safeguarding their privacy.

A study on cyberbullying carried out by Li (2006), involved a similar number of respondents to the work presented in this thesis (264), and these were of a similar, although not directly comparable age (13 to 15 years old). Nonetheless the contents of this study are relevant for comparison with results obtained. These results included levels of understanding of the term, and the experience of cyberbullying by gender.

Badenhorst (2011) published a report on the legal aspects of the consequences of these behaviours within the South African context. Additionally examples of sexting and cyberbullying that occurred in South Africa were discussed, including their legal outcomes. This report is included in Appendix A.

Relevant to privacy and sexting is a 2008 survey conducted by the (American) *National Campaign to Prevent Teen and Unplanned Pregnancy* in conjunction with *Cosmopolitan Magazine* (The National Campaign 2008). This covered a larger age range of respondents (ages 13-26) than those included in this research (ages 16-18), but incorporated the relevant age range, and also divided the larger group into results based on the categories of 'teen' (ages 13-19) and 'young adult' (20-26). The former category is most relevant, and while the results are not wholly comparable in terms of age, they nevertheless make for an interesting comparison in terms of findings as discussed in Section 6.1

Another survey, by Rice, Rhoades, Winetrobe, Sanchez, Montoya, Plant, and Kordic (2012) asked questions relating to sexting. The age range of their respondents, 14-19 years old is comparable to a point with the target group of this research. Similarly, a survey carried out by Microsoft in July 2011 (Microsoft 2011) dealing with the online

reputation of 13-17 year olds makes for interesting and relevant comparison with the research at hand owing to the coverage in it of issues relating to online privacy and social media . Findings of this research also indicated levels of concern and interest relating to online privacy, while also providing some details of what was regarded as important in terms of protection.

Marwick, Murgia-Diaz and Palfrey (2010) carried out a literature review in which the focus was also on youth privacy and reputation. This covered some of the issues addressed in this research, albeit at a deeper level, and using a wider age range of subjects (13 to 19 years old, with reference to younger groups as well). This review provided results that young people within their respondent age rage were more concerned about their online privacy than was assumed, noted that females were likely to be more so, and also noted the willingness of their subjects to engage with stranger online.

2.4 SUMMARY

The literature, and studies discussed in this chapter provide some insight into the broad area being researched, as well as some of the thinking and outcomes around it. The material in covered in this chapter also assists in placing this research into context though comparative studies. Finally, relevant terms were defined to provide the reader with an understanding of the terms and concepts as used in the discussion of the results of this research.

CHAPTER 3: RESEARCH DESIGN

The purpose of a research design is to serve as a "…strategic framework for action that serves as a bridge between research questions and the execution or implementation of the research" (Durheim and Terre Blanch 1999:29). In essence this section provides the link between the goals of the research as stated in Section 1.3 and the research carried out. The process leading up to the implementation of the research is described in detail. The construction of the questionnaire is also discussed, as is the research methodology used. The deployment of the questionnaire within the schools is also described.

Taken into account in the design is the principle espoused by Sellitz cited in Gable (1994) that when planning research is it necessary to ensure as far as possible " … the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy of procedure." This principle guided both the selection of the target schools in terms of geographical proximity, (see Section 3.1) and the use of an electronic questionnaire as the method of gathering data (see Section 3.3).

3.1 SELECTION OF SCHOOLS

As outlined in Chapter 1, the target group were school learners, in the 16 to 18 years old age bracket with regular access to both computers and/or cellular telephones, and the Internet. The next steps therefore were to work out which schools should be contacted, how best to do so, and the most appropriate methods of, and approaches to, data collection.

Since the research was being carried out in Grahamstown, it was necessary to consider schools based in this location. This was because of the possibility of having to meet with Principals or other school representatives, and also the originally proposed idea of following up a possible questionnaire with a once-off interactive session at each school (see Section 3.3).

Schools considered for approach were School A (male learners only), School B (female learners only), School C (male and female learners), School D (female learners only), School E (male and female learners), and School F (male learners only). These schools were considered based on the facilities at the schools, and the gender mix required to fulfil one of the research goals. While the facilities provided, namely computer laboratories, were a major factor in the consideration of these schools, so too was the greater possibility of learners at these schools having access to personal computing and telephonic facilities, as well as having access to such facilities at home than may have been the case at less well funded schools in the area. Knowledge of the computing facilities offered by these schools came from living and working in the geographical area, and having occasional contact with staff members as a well as past learners of the relevant schools over a number of years.

Prior to any action being taken on approaching these schools, the computer lab at School E was badly damaged in a fire. As a result, the decision was taken not to approach this school regarding involvement in the research study. Therefore the decision was taken to formally approach School A, School B, School C, School D, and School F.

3.2 DATA COLLECTION PROCESS

Contact with the Principals of these schools was made via email in order to gauge interest in participation. This email message (individually sent and personally addressed) consisted of a number of parts, the first being a statement of who the request was coming from, and under whose auspices i.e., the names of the university, department, and research supervisors. The next part was a brief outline of the intended area of study, which included mention of cyberbullying. Whilst the research was always intended to have some degree of focus on cyberbullying, this area was mentioned specifically in the first contact with the schools, in order to emphasise the relevance of the research to their particular schools and encourage willingness to participate. Following this in the email was a request that if there was interest from the school, that the Principal indicate so, or appoint a representative do to so. This email concluded with contact details of the sender, and the expressed willingness to entertain questions if required, or meet in person if preferred.

An immediate response was received from the Principal of School A, with a statement of interest, and willingness to participate, as well as the naming of the representative who would oversee the involvement of the school. Following this reply, contact was made by his designated representative, the Vice-Principal, requesting a meeting. At this meeting a section on the goals of the research was extracted from the Research Proposal and provided to the representative in hard copy. The participation of this school was confirmed and contact established regarding potential timeframes and the possible logistics of the learners' participation.

Similarly an enthusiastic response was received from the Principal of School B, who also named a Vice-Principal as a representative for dealing with the school's involvement. In time, contact was established with this representative, and no meeting was requested. The same extract from the Research Proposal as provided School A was provided electronically to the representative from School B. The response from the Principal of School D was very enthusiastic, and he elected to be personally responsible for the school's participation process. Although no meeting was requested, the aforementioned proposal extract was sent on. The Principal of School C also replied enthusiastically, and also appointed a Vice-Principal to be his representative in terms of managing the participation of the school. Contact was made with this representative, and as with the other schools above, the proposal extract was sent via email, with no meeting was requested by the representative.

No response was received from School F. Consideration was given to follow-up, but after a period had elapsed during which the other schools had begun their participation, with no response received, the decision was taken that the absence of this school would not have a negative effect on the survey being carried out. This was based on the large number of completed questionnaires from the other schools by that stage.

At this point, the issue of participant consent needed to be taken into account before continuing. Complicating this was the fact that minors were required to take part in the survey. Three of the schools are Independent Schools, and primarily boarding schools. As such, the school Principals were able to act in *loco parentis* and provide consent for their minor learners to participate. They were also able to provide permission for their individual schools to be involved in the research. Learners 18 years and older were of

course able to consent themselves. School D is a government school, and as such the Principal made it known that the Department of Education needed to provide permission for the school to participate, before he could allow the research to take place. Consequently logistical discussions with this school were placed on hold, prior to the outcome of contacting the Department of Education District Office.

Communication with Schools A, B, and C continued, and during this time a draft questionnaire was sent to each of the school representatives. This was to provide them with a better idea of what their learners were undertaking, and to give them an opportunity to express any concerns with the subject matter being covered, or over any specific questions. All three participating schools sent the draft questionnaire back without queries or recommended changes. Discussion regarding the estimate of numbers required took place, with initially between thirty and fifty learners requested to take part at each school. Later on this request was amended to include as many learners as possible without causing undue disruption to the programmes of the participating schools.

Once the questionnaire had been finalised (see Section 3.3), it was necessary to gain ethical clearance from the Ethics Committee at Rhodes University, as the research would involve people. An ethical clearance form was submitted to the aforementioned committee for approval. Included in this application were the emails from the school representatives providing consent for their learners to take part. Ethical clearance was subsequently obtained.

Once the questionnaire had been finalised, it was once again sent electronically, in Portable Document Format rather than as a URL, to the representatives of the participating schools, and discussion began in earnest regarding the final logistics of learner participation. As the decision had been taken from the conception of the survey to make it online rather than paper-based, the appropriate link for each school was supplied to the relevant school IT representative (based on contact with the aforementioned schools). The way this was used by the schools is described in Section 3.3.

An initial logistical hurdle at School A and School B, was that the online nature of the questionnaire required the learners to use the computer labs, which in turn could not accommodate enough learners at the same time to complete the questionnaire in one sitting. This was overcome as follows: School A and School B put similar arrangements into place: At School B, learners in Grades 10 to 12 took turns over three consecutive weeks, during a forty five minute designated 'tutor period', with one grade per week filling out the questionnaire. At School A, a similar exercise was done, but the participants were grouped by boarding house rather than grade. As such while the majority of learners in each grade were exposed to the survey at School B, at School A it was approximately half of the learners in each grade. No formal arrangements were made by School C other than a letter to all learners in Grades 10 to 12, from the Vice-Principal requesting them to answer the questionnaire and providing the school-specific URL. Nonetheless the response was impressive in terms of completed questionnaires at this school, and the other two schools.

Whilst the survey was in process at the other schools, attempts were still being made to contact the Department of Education District Office. Numerous attempts over a period of weeks to establish contact via telephone and email were unsuccessful. Subsequently a letter and a copy of the questionnaire were hand delivered, and the promise of feedback within a week received. Subsequent attempts to follow up on this via telephone and in person were unsuccessful. By this stage 258 completed responses had been received from the three participating schools, and the decision was made, regrettably, to inform the Principal of School D that due to time constraints, it would not be possible to include the school in the study. At this point, the information gathering section of the research was considered complete. At the time of writing no response from the Department of Education District Office has been received.

3.3 QUESTIONNAIRE DEPLOYMENT

As noted in the introduction to the chapter, it was decided that the most appropriate method of gathering the required data would be to use a questionnaire. Reasons for this include: the flexibility of a questionnaire in terms of gathering both qualitative and quantitative data (see Section 3.5); the anonymity offered by a questionnaire compared to any form of interpersonal interactive contact with research participants; the

potential ease of distribution; and the relative economy of time required from participating schools for their learners to take part in the research. Cohen, Manion, and Morrison (2011:91) state that "…the essence of anonymity is that information provided by participants should in no way reveal their identity." This criterion was met with no *personally identifying* data collected during the course of the research. Anonymity was considered an important aspect of the research, as it was felt that participants would be more likely to provide truthful answers knowing that these answers were not going to be examined by the school, or traced back to them personally.

It was originally planned to follow up the participation in the questionnaire with an interactive session with respondents at each of the schools. The aim of doing this was the possibility of gaining further insight into the information collected through the questionnaire. As the schools had already provided much assistance in terms of allowing, and arranging for their learners to participate, it was decided that pressing them for further involvement would be unnecessary and this follow-up idea was abandoned.

The decision to make use of an online rather than paper-based questionnaire was taken on the basis of avoiding the printing and manual data capturing inherent in paper based forms. Following Cohen et al. (2011), online questionnaires have a further advantage over paper based ones in that many of the options available for creating them also include automatic collation and results presentation features. It was also felt that distribution to the schools would be easier, and the time taken for each learner to complete the questionnaire would be less than if a paper-based survey was used.

Several options for appropriate software were investigated, with the major criteria being ease of use, unlimited respondents, and little or no charge. *Limesurvey* (www.limesurvey.org) met the criteria, and although not as simple as other options to set up, proved to be the most appropriate candidate. Installation on an active web server was required, and once this was done, the construction of the questionnaire was able to move from rough draft towards completion.

Once the first online draft was completed, it was decided that each school should have their own unique URL and accompanying database. This was to prevent instances of respondents from one school pretending that they were from another, and to enable

separate databases to be kept for each school. It should be noted at this point that in the initial correspondence with the Principals of the schools, it was communicated that the individual schools would receive feedback on the responses from their learners, as well as the overall responses at the conclusion of the research.

At Schools A and B, the URLs were placed on the respective intranet pages of the schools. At School C, the URL was sent out to the learners in an email (by the school representative), and was accessed directly off the Internet. It should be noted that prior to the engagement of the respondents with the questionnaire at each of the schools, the following informational piece was distributed to the schools, for advertisement to the respondents prior to commencing their responses:

'Instructions to participants prior to commencing the questionnaire

• Permission has been granted by your School Principal for you to take part in this survey

• Your name and contact details are not asked for and as such your participation is ANONYMOUS, so please answer freely

• Individual responses will not be distributed to anyone

• The collective responses both from your school and from the other participating schools will be provided to your School Principal.

• Several questions are marked as mandatory, so you will need to answer them before you are able to proceed to the next question [these related to consent, age, Grade and gender]

• Please read the instructions to each question carefully

• Please answer all questions

• The purpose of this survey is to assess your awareness of online threats, and online behaviour patterns, with a view to providing useful feedback in terms of online safety.

• Thank you very much for your participation '

Worth noting too when examining these instructions is that they were informed explicitly that permission had been granted. For discussion of possible disagreement with this statement by respondents, see Section 3.4. Furthermore the anonymity of participation was again made clear, and emphasized in light of any potential misunderstandings from respondents regarding the provision of *collective* results to their schools. The standard request to answer all questions was felt necessary in order to encourage participants into responding with the mind-set of fully completing the questionnaire. Options regarding mandatory questions are discussed in Section 3.4, and the remainder of the pre-response information simply emphasizes the subject of and reasons for the existence of the questionnaire and their participation.

3.4 QUESTIONNAIRE DESIGN

It was decided that grouping the questions into related sections would be preferable to having a single set of questions. The reason for this was twofold: firstly grouping the questions made logical sense from a questionnaire design and layout perspective, and secondly, the intention was to provide additional clarity to the respondents in terms of what they were answering. Taken into consideration was the assumed likelihood that not all respondents would be familiar with the terms and concepts covered by the questions, and that grouping the questions into clearly labelled blocks, with guiding principles would assist in providing additional clarity.

Prior to encountering the questions, once given the URL for the questionnaire, the respondents would be presented with an initial message stating (with the appropriate date for each school): 'Online Information security Threat Awareness and Behaviour Questionnaire: The purposes of this questionnaire are to assess the awareness of online threats to information security, and to determine online behaviour patterns in school learners with access to the relevant technology in the Grade 10 to 12 bracket. This Survey will be active from midnight 13/05/2012. There are 98 questions in this survey. While the questions were numbered up to 100, the insertion of the acknowledgement of Principal consent, and the removal of another question prior to deployment meant that in fact only 98 questions were answered. The question numbers as shown in Appendix B correspond with the numbers of the questions referred to in the discussion.

The informational message quoted above was included to reinforce the purpose of the survey to the respondents, and to let them know from the beginning the number of questions so that they would be aware of what the end point was. This message complies with a principle espoused by Witte, Ambrosio and Howard (1999:139) that questionnaire introductions should be "short … informative … and avoiding (of) giving a long list of instructions". No suggested timeframe for completion was provided as control of time allocated for answering was in the hands of the participating school.

While the questions were divided into the various sections, several concepts and issues were incorporated into more than one section. The purpose of this was to provide a check for consistency of response, and understanding across the sections. It also holds true that the lines between information security and online privacy are not clearly defined, and there is, or can be, significant crossover between these areas. This crossover is clearly evident in the questions across the different sections. To an extent the grouping was also done to provide convenient blocks for both for the respondents while answering and later analysis.

Initially the intent was to make all the questions mandatory, with the respondent not being able to move forward to another question without answering the preceding one. This was reconsidered in terms of allowing the freedom of choice for respondents to answer only those questions that they wished. Dillman, Carley-Baxter and Jackson (1999) address this issue of mandatory questions with the suggestion that options not requiring an actual answer be provided. Following this advice, and the concern that allowing questions to be skipped would result in a significant number of incomplete surveys, it was decided to make the majority of questions mandatory, but to introduce a 'Not Applicable' option to most the of the questions. This option would allow people to whom the question was not applicable to select this option, and then to skip the following question, which in many cases was a follow up. These follow up, or 'expand on the previous answer' questions were not set to be mandatory. It was intended that setting up the questions in this fashion would avoid antagonising respondents resulting in abandonment of the survey as warned by Cohen et al. (2011), while still allowing them the choice to not provide answers to questions if they felt strongly about doing so.

Consideration was given to structuring some of the questions in a manner allowing respondents to skip to certain questions based on answers given on previous questions, an approach favoured by Redline, Dillman, Carley-Baxter and Creecy (2003). Ultimately it was decided that it was better to avoid this approach and rather simply have the aforementioned 'Not Applicable' option instead for most questions. In some cases (where the 'skip to this question depending on the answer just given approach' may have been used) the question begins 'if you answered 'yes' to the question above …', and then provides the option for a 'Not Applicable' answer. This approach is backed by Cohen et al. (2011) who suggest that a risk of allowing respondents to skip to questions is that questions that would otherwise have been answered could be inadvertently overlooked.

The structural makeup of the questions was decided upon to be primarily multiple choice answers, where options could be selected from a drop-down list or panel of radio buttons. In some cases more than one selection was required to answer a question, or was made an optional manner of answering the question. The reason for this as a primary structure was for ease of data capture and interpretation. Dillman et al. (1999) suggest that in web-based surveys it is advisable to avoid the presence of large number of open-ended questions, and to rather make use of drop-down lists or radio buttons for ease and efficiency of data and quantitative analysis. The structure of the questionnaire conforms to this viewpoint. For several questions however, the requirement was to provide a written answer. The purpose of questions such as these was to allow for freedom of responses to these specific questions, or to provide the opportunity to elaborate on answers to other questions. It was decided that there were places where open-ended questions were important to gain deeper insight into some of the answers given by the respondents. The sections of the final questionnaire are discussed below:

3.4.1 PREAMBLE

This section consisted of a single option, for the participant to acknowledge whether they were aware that consent had been given by the school for them to take part in the survey, and complete the questionnaire. This option also provided opportunity for the student to acknowledge that they were aware of the personal anonymity (see Section 3.3) regarding their participation. It is acknowledged both in principle and on the

application for ethical clearance to conduct the research that the respondents may have been placed under direct instruction by the schools to take part in the research. This was not regarded as overly significant, as respondents still had the choice to answer the questions or not. This was because no way (other than through visual inspection perhaps) existed for the school staff (if any) monitoring the respondents' participation to be aware of whether a questionnaire was complete, partially complete, or entirely incomplete. In practice some incomplete questionnaires were received, but whether this was a function of limited time provided for answering or for other reasons remains a matter of conjecture.

3.4.2 SECTION A: DEMOGRAPHICS AND BACKGROUND

The purpose of this section was to gather information about the participants, which would assist in forming profiles of the respondents. These profiles would be based on establishing details such as age, grade, gender, access to computers, cellular telephones and the Internet, frequency of access, and perceived awareness of threats. The purpose of the questions was therefore to provide baselines in terms of the respondents' (limited) personal details and access. These baselines would then be used for comparisons and correlation with data from the remaining sections of the questionnaire. As per the decision noted previously regarding anonymity of participation, there was no request for the respondents to provide their name, other identifying information, or any personal information other than the aforementioned age, grade, and gender.

Cohen et al. (2011:91) state that "A participant is therefore considered anonymous when the researcher or another person cannot identify the participant … from the information provided." As this was indeed the case it can be said that the conditions of anonymity were met during this research, and the privacy of the respondents (perhaps especially important considering the subject of the research) was guaranteed. This section contains the first sixteen actual questions of the survey.

3.4.3 SECTION B: SOCIAL MEDIA

The questions in this section relate specifically to the use of social media by the respondents. The first half of these questions were intended to provide insight into which social media applications were used by the respondents, the amount of time spent using these, and their reasons for making use of social media applications. One question addressed their concerns and perception of any negatives or disadvantages of the use of social media. The remainder of questions in the section sought to gain insight into the respondents' behavioural use of social media, and in particular their interactions (or lack thereof) with persons unknown to them other than through online means. Elements of this section link up with Section 3.4.5, but in this section the focus is strictly on social media. Cohen et al. (2011:277) hold the view that "…as the first question in a survey tends to raise in the respondents' minds a particular mind-set, care is needed to entice participants and not put them off participating." As such, this section, which contains the first actual informational questions, is placed where it is, as it was assumed (see Section 1.5) that respondents within the defined age range would be familiar with social media, owing to everyday use, and would therefore feel immediately comfortable in answering the questionnaire. Questions 17 to 35 make up this section.

3.4.4 SECTION C: DIRECT AWARENESS OF THREATS

The focus of the questions in this section were intended to address the actual awareness of known threats to online privacy and security, ranging from the commonly known such as viruses, to the more obscure, for example browser poisoning. Basic issues were raised, such as awareness of anti-virus software and operating system updates. There was further self-assessment of awareness levels, as well as questions intended to begin the process of gaining insight into respondent behaviour while online. The latter included some questions that would also have fitted easily into Section 3.4.5, but were considered more appropriate in this section under direct awareness of threats; for example, a question on whether the respondent had been approached with a request for any personal details. Behaviour-based threats were also introduced; for example, a simple question on whether the respondent had clicked on an attachment in an unsolicited email. This section is made up of Questions 36 to 50.

3.4.5 SECTION D: BEHAVIOUR AND PRIVACY

This section comprises Questions 51 to 75, and was designed to focus more deeply on the subject matter of its title. Questions are asked on specific privacy based options and awareness, including the area of social media. The purpose of these questions was to gain insight not only into what the respondents know, or perceive themselves to know, but also their actions in terms of this knowledge. Included in this section are questions seeking to interrogate password habits and behaviour, as well as actions taken with regard to privacy settings across various applications and circumstances. It was intended that questions in this section would provide further insight to answers in the preceding sections.

3.4.6 SECTION E: USER EXPERIENCE

This section comprises the final 36 questions in the survey, 76 to 100. The questions in this section were designed to deal further with the respondents' experiences online, in terms of their interactions with strangers and peers. As with previous sections there are crossovers between questions in this and other sections in terms of larger subject areas. Questions were included which sought to investigate the respondents' actions and reactions to various online situations. For example a focus on cyberbullying was included in this section, as well as questions relating to the overall themes of information security and online privacy, and respondents' experiences with explicit material in terms of transmission. The intent was to assess this within the context of online privacy, rather than as part of a more general delving into online behaviour relating to explicit material, although the significant risk posed by such action led to a greater focus on this (see Chapter 6).

The survey concludes with the final two questions asking if the respondents has heard of the South African Electronic and Communications and Transactions Act (2005), and whether or not they had found participating in this survey useful in terms of increasing their awareness of information security and online privacy. These two questions, while included under this section, are not strictly a part of it, and were intended merely to conclude the survey. The latter question was included specifically for comparison with answers received, during post survey data analysis, in order to match perceived knowledge with the value drawn from taking part in the survey.

3.5 METHODOLOGY

Following the decision to conduct the study through the use of a questionnaire, this questionnaire was designed to gather data in a primarily quantitative manner but also to include a small number of qualitative questions. The information gathered in this survey was then used to compare and contrast results from the questionnaire with relevant surveys or studies noted in the literature survey.

3.6 DEMOGRAPHICS, BASELINE INFORMATION AND USAGE PATTERNS

The information collected in this section is intended to establish a baseline of information about the respondents. This was to ensure that the demographic information collected about the respondents was correct in terms of the research goal.

Analysis in this section and in all subsequent chapters is performed using the options available in the *Limesurvey* software used to collect the data, as well as *Microsoft Excel*, and the '*R*' statistical software package. Whilst the data was analysed on its own merits, the results occasionally make for interesting comparison with the assumptions made prior to the research being carried out (see Section 1.5). This is noted and discussed as appropriate. Data analysis was performed based on overall themes to which answers were sought. As such, and owing to the large volume of data collected, not every question, and not every possible combination of data is analysed.

Of the responses received, it was decided that only complete responses would be analysed. As such 258 responses were considered in terms of results and discussion. While the survey was carried out with separate databases for each of the participating schools, for the purposes of analysis the collected results were combined. It is acknowledged that lack of familiarity with some of the terms could have had an influence on the answers received from the respondents. Where appropriate, this is noted. Comparisons with other work are introduced throughout the discussion chapters as appropriate.

3.6.1 BASELINE INFORMATION

As noted above, 258 completed responses to the survey were received. Of these, 122 (47.29%) were from male respondents, and 136 (52.71%) were from female respondents. In terms of the stated goal of investigating potential differences between the genders, the relatively even split between the genders of respondents was a useful result in terms of later gender comparisons. Further, 70.93% of the respondents declared themselves boarders at the school, compared to 28.29% as day learners. The remaining 0.78% (all of two respondents) declared themselves 'other' (in both cases they specified 'private boarder', which is a learner who lives with another family rather than in one of the school boarding houses. This split was as expected, considering that the schools participating in the survey are primarily boarding schools.

The age range too was compliant with what was expected of learners in the target bracket of school grades 10 to 12, with an average age of 16.43 years recorded. The minimum age entered was 14 years old (consistent with a Grade 10 learner who is a year young for their grade, in that they will turn 17 rather than the usual 18 in Grade 12), and the maximum age was 18 years old, which is consistent with the age reached of the majority of learners in their Grade 12 year. All respondents were in the correct grade range, but as the intention of the research was to assess the respondents as a homogenous group rather than on a per grade basis, analysis according to grade breakdowns was not carried out. The initial analysis served purely to confirm that the correct Grades took part in the survey.

The target group of the survey was learners with *regular access to computing facilities, the Internet and cellular telephones*. In order to establish that this was the case, the questions in Section A of the survey focussed on establishing a baseline of respondent access and usage. Here, 87% of the respondents indicated that they had access to a personally owned computer (of varying descriptions), while all respondents indicated that they had regular (three or more times per week) access to computing facilities (including those that were not their own).

In addition, of the 258 respondents, only one indicated that they did not own a cellular telephone. When queried as to whether access to the Internet was primarily via cellular telephone or computer, the answers were split 63% to 59% in favour of access via

computer (many respondents selected both options), and those who selected the 'other' option indicated 'both' as their response. These responses were interpreted as indicating that the respondents made frequent use of both methods of accessing the Internet, with no absolute preference. It could therefore be concluded that the respondents met the desired criteria as a target group in terms of grade, age, access to computing facilities, and the Internet.

3.6.2 USAGE PATTERNS

Having determined the suitability of the group in terms of the research criteria, above, it was necessary to gain further insight into their actual engagement with the online world available to them. The information was drawn from Question 16.

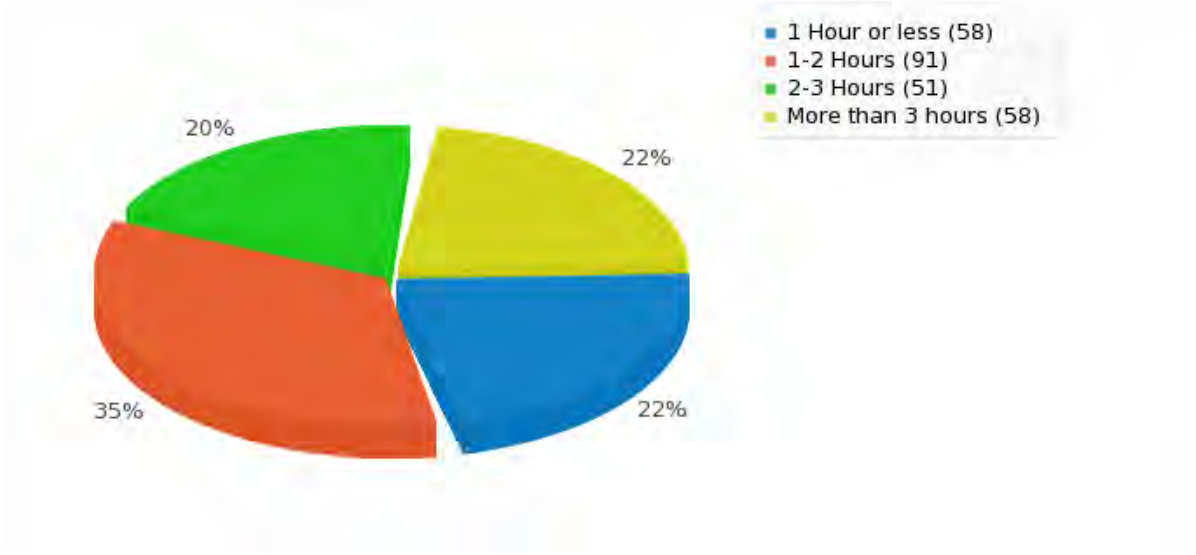

Figure3.1: *Self -assessed number of hours per day spent using a computer or cellphone to access online services (including the Internet, text and instant messaging)*

As is apparent in Figure 3.1, the greatest number of respondents spent 1-2 hours per day accessing online services. By combining these figures however, it is shown that 109 respondents or 42.24% spent two or more hours per day, while 200 respondents, or 77.57% spent at least one hour or more per day.

***Table 3.1**: Self-assessed number of hours per day accessing online services*

Usage category (Hours per day)	Male (n=122)	%	Female (n=136)	%	p-value
1 Hour or less	36	29.51	22	16.18	N/A
1-2 Hours	46	37.70	45	33.09	N/A
2-3 Hours	23	18.85	28	20.59	N/A
More than 3 hours	17	13.93	41	30.15	N/A
Total of categories 2,3 and 4	86	70.49	114	83.82	0.017*

** significant at the 5 % level*

Table 3.1 reveals the breakdown of these results by gender. The bottom row in this table is the sum of respondents whose answers fitted into all the categories of 1-2 hours or longer per day. A Student's' t-test was then conducted using the 'R' statistical package on this last row to determine whether the percentages indicating that female respondents had a higher usage level was significant. The result of this ($p=0.017$) indicated that it was statistically significant at the 5% level that female respondents spent more time per day accessing online services than their male counterparts. This in itself is not necessarily indicative of anything. Viewed in the context of Chapter 4, dealing with the awareness of threats however, it is revealed that female respondents were less aware to varying levels of statistical significance of certain online threats. Thus owing to a higher amount of daily online activity, and a lower awareness level (as determined in Chapter 4), female respondents could be slightly more at risk, as the more time spent online could be equated with greater time with exposure to and/or interaction with threats.

Since social media and the use thereof was included in the questionnaire as a major component, it is worth establishing the respondents' actual usage behaviour. As such, further to the levels of usage in Table 3.1, the respondents' estimations of their frequency of use of social media, and their total time spent was assessed through Questions 20 (usage per week) and 21 (usage per day). A total of 83.72% of the respondents fell into the category of accessing at least one social media platform or application *daily*. Male (83.60%) and female (83.82%) figures were remarkably consistent with this overall figure, and showed an almost identical pattern of behaviour between the genders.

Question 21 asked respondents to estimate the amount of time spent using social media out of their total time spent using the Internet. This was specifically phrased to be clear that it was referring to the Internet rather than general online connectivity. Results indicate that 32.17% was the highest figure recorded for a single category. This is the category which indicated that respondents spent *approximately half* of their time on the Internet using social media.

With just one category available for selection indicating that *less than half* of their total time was spent on social media providing a figure of 27.52%, the other categories were added together to produce the figure that 74.41% of respondents spent *half or more* of their total Internet time on social media, with 23.64% admitting to spending *most* of their Internet time in this way. This figure was indicative of the sheer volume of time spent in this way; time which would potentially have been, as discussed in Chapters 5 and 6, time spent under threat.

3.7 SUMMARY

Covered in this chapter were the selection of the respondents and the processes involved in the collection of data. Also covered were the research methodology and the construction of the questionnaire itself. In closing the baselines for the respondents were assessed, and found to be correct in terms of the stated research goals. The following chapter contains the first discussion of the results of analyses performed on the collected data.

CHAPTER 4: AWARENESS OF THREATS

Awareness of threats was investigated by asking respondents to indicate their perceptions of their own awareness levels and by posing questions later on in the survey which required respondents to reveal their actual awareness levels by identifying and defining threats. The purpose of this approach was to provide a check on perceived versus actual awareness. Respondents were unable to return to previous answers, and as such were unable to 'raise' their perceived awareness level following exposure to information presented later on in the questionnaire.

4.1 SELF PERCEPTION OF AWARENESS

Through Question 14, an assessment was made of the respondents' self-perceived overall awareness of software, the Internet and other threats to online information security and online privacy, in general terms. The results are shown in Table 4.1.

***Table 4.1**: Levels of perceived awareness*

Awareness level	Total % (n=258)	Male (n=122)	Female(n=136)	p-value
Very aware	32.95(n=85)	38.54(n=47)	27.94(n=38)	0.072
Moderately aware	52.71(n=136)	47.54(n=58)	57.35(n=78)	0.116
Generally unaware	12.40(n=32)	11.47(n=14)	13.23(n=18)	0.669
Very unaware	1.94(n=5)	2.45(n=3)	1.47(n=2)	#

 # p-value not calculated due to small sample size

Given the choices, 32.95% of respondents regarded themselves as 'very aware', 52.71% regarded themselves as being 'somewhat aware of the terms and issues' (indicated as *moderately aware* in Table 4.1) and 12.4% regarded themselves as 'having heard of some of these (terms) but not being quite sure what they mean' (indicated as *generally unaware* in Table 4.1). Five respondents, or 1.94%, regarded themselves as *very unaware*. The majority of the respondents therefore considered themselves to be at the very least moderately aware of threats to information security and online privacy.

This is an expected result, taking into account the frequency of computer, (cellular) telephone, and Internet use evident amongst the respondents. A Student t-test was applied to each of the first three categories in this table to determine the statistical significance of the apparent gender differences, if any. As indicated in Table 4.1, none of the p-values revealed any significant statistical differences between the answers of male and female respondents.

To gain a better *overall* impression of the perceived awareness levels of the respondents at this point, the *moderately aware* and *very aware* categories were combined, to provide a figure of 221 respondents, or 85.65%, who regarded themselves as 'aware', as opposed to only 14.34% who fell into the combined category consisting of *generally unaware* and *very unaware*. While the figure of 85.65% appears high it should also be noted that this figure purely reflects *perceived* awareness, not actual awareness in any sense, as is determined later.

When this figure of 85.65% of 'aware' respondents is broken down by gender, the responses show that 85.29% of female respondents regarded themselves as being 'aware', (the combined numbers of *very aware* and *somewhat aware*, as above) compared to 86.06% of male respondents. These figures are, unsurprisingly in gender terms, considering the p-values already displayed, consistent in terms of a lack of statistically significant gender difference. From this it can be inferred that in terms of self-perception of awareness, that overall, based on numbers, percentages and statistical confirmation via Student's t-tests, there is no reason to conclude that either male or female respondents *regarded themselves* as being more aware than the other. This is a result that bears further scrutiny in terms of a comparison between these perceived awareness levels and results obtained from questions intended to gauge the accuracy of the respondents' perceptions.

4.2 AWARENESS IN RELATION TO PERCEPTIONS OF IT

In Question 36 the respondents were asked to indicate which online threat related terms, chosen from a list, they had encountered. Considering the subject matter of the questionnaire, and the depth of this question therein, it was assumed that respondents would place these terms within the correct context. This may not have been the case

with all of the terms provided, specifically social engineering, and spoofing, as these are terms that appear outside of the framework of information security as well. The remainder of terms fall squarely within the realm of information security. The word 'encountered' was not pre-supposed to indicate an in-depth knowledge of the terminology, but was intended to assess awareness at the lowest level possible: that of simply having come across a term before, or casual understanding at best.

Table 4.2: *Recognition of Terms*

Threat Term	n=258	Total %	Male %	n=122	Female %	n=136	p-value
Phishing	52	20.15	27.04	33	13.97	19	0.009**
Identity Theft	95	36.82	42.62	52	31.61	43	0.068
Social Engineering	35	13.56	18.85	23	8.821	12	0.020*
Smishing	5	1.93	2.45	3	1.47	2	0.573
Vishing	7	2.71	4.09	5	1.63	2	0.207
Keystroke Logging	30	11.62	17.21	21	6.61	9	0.009**
Spam	117	45.34	50.81	62	40.44	55	0.095
Computer Virus	163	63.17	70.49	86	56.61	77	0.020*
Online Privacy	123	47.67	49.18	60	46.32	63	0.648
Cybercrime	67	25.96	31.96	39	20.58	28	0.039*
Crimeware	40	15.50	22.95	28	8.82	12	0.002**
Malware	60	23.25	31.96	39	15.44	21	0.001**
Spyware	88	34.10	46.72	57	22.79	31	<0.001***
Trojan	63	24.41	31.96	39	17.64	24	0.008**
Computer Worm	70	27.13	32.78	40	22.05	30	0.054
Spoofing	28	10.85	14.75	18	7.35	10	0.060
Browser Poisoning	16	6.20	8.19	10	4.41	6	0.216
WSUS	4	1.55	1.63	2	1.47	2	0.913
419 Scam	10	3.87	5.73	7	2.20	3	0.153
None of the Above	50	19.37	16.39	20	22.05	30	0.249

** significant at the 5% level;** significant at the 1% level; *** significant at the 0.1% level*

The results obtained allow for interesting comparison with the perceived awareness levels above. Table 4.2 gives the breakdown of these results according to gender, and as percentages of the total number of responses. Selected terms are expanded upon in terms of respondent behaviour, risk to the respondents and potential impact. As appropriate these results were tested for gender significance at a statistical level, and the results discussed, and an overall conclusion around the awareness levels of the respondents is presented.

Upon examination of Table 4.2, it is apparent that according to the percentage breakdowns, in all cases the female respondents displayed less familiarity with the terms than their male counterparts. In the majority of cases, with the exception of online privacy where there is a 2.85 % difference, of the terms that were recognised by more than 10% of all respondents, the female responses are between 7 and 23% lower than the male ones, with an overall average of 8.7% lower awareness. This finding is consistent with the discussion in Section 4.1 where 57% of female respondents indicated their unfamiliarity with threats generally, while noting that they had encountered some of the terms before.

While these percentages provide an indication of possible relevance, tests for statistical significance are necessary before drawing firm conclusions on gender performance. A Student's t-test was conducted on each of the terms, for gender significance, and as shown above, in 9 of the 20 terms ('none of the above' is excluded), there are statistically significant gender differences. In all cases, the bias is in favour of the male respondents showing more actual awareness than their female counterparts. While this is not necessarily conclusive evidence of an overall pattern of higher actual awareness levels amongst males, it is worth noting owing to the aforementioned bias towards males in all areas showing a statistically significant gender difference, and potentially indicative of a trend towards superior male awareness. This is in contrast to the perceived awareness results, where no significance was noted for the differences in responses between genders.

Thus based on the results of analysing Table 4.2, it could be concluded that both male and female respondents perceived themselves to be more aware than their actual results indicate in terms of threats, and that there is a slight bias in favour of male actual

awareness. This higher level of awareness for males occurred predominantly in terms that may be considered less mainstream in terms of media coverage, unlike viruses for example. These terms include phishing (which has gained notoriety to the point where it may be considered as common a term as virus), keystroke logging, social engineering, cybercrime, crimeware, malware, spyware, and trojans. The final inference that could be drawn from this is that while there is no outright significance in the difference between male and female respondents in terms of awareness, the exceptions indicated that males had a higher level of knowledge / familiarity with the more obscure or less common terminology, and therefore an overall edge in awareness levels over the female respondents.

4.3 EXAMINATION OF TERMS AND RISK

It is evident from Table 4.2 that, the term most often encountered, unsurprisingly, was 'computer virus', which was anticipated to have the highest rating, owing to the ubiquity of both the term and what it represents. What is surprising however, is that only 63.17% of all respondents indicated that they had encountered this term. Notably in this instance there is a statistically significant gender difference at the 5% level in favour of male respondents, in recognition of this term. As was demonstrated (in Section 3.6.1), the respondents all had regular access to computing facilities, with the majority having access to personal computers. This was therefore not only a surprising result, but an indicator of a potentially serious flaw in the respondents' awareness of the threats to the very machines they use regularly. It is unsurprising that responses to Question 38, which enquired as to whether the respondents had been infected by a virus, indicated that 49.61 % of respondents' computers had in fact been infected by a virus.

While there were no 'non answers' and the percentage of respondents indicating that their computers had not been infected by a virus stood at 50.39%, considering the data in Table 4.2, it could be suspected, if not presumed, that there had been more infections, of which respondents in the 'no' category had simply not been aware. The assumption in this last sentence is further validated by the responses to Question 39 (If the respondents had been infected by a virus, were they aware of how this had happened?). Answers to this question indicated that of those admitting to having had a computer

virus infection, 56.8% also admitted to not knowing how their computer got infected. As observed above this is a serious flaw in the awareness levels of the respondents, and thus a serious security risk to the respondents, and by extension others, owing to the nature of virus propagation.

Looking more deeply at the relationship between awareness and infection via Table 4.3 (drawn from the answers to Questions 36, 38 and 39), the first row, *awareness,* shows respondents who had indicated that they were familiar with the term 'computer virus'. *Infection* shows those respondents who had answered that their computer had been infected by a computer virus. *Aware and infection* denotes those respondents who had indicated their familiarity with the term and admitted to having had a virus infection on their computer. *Unaware and infection* shows respondents whose computer had been infected *and* who had indicated that they had not encountered the term. *Aware and cause unknown* shows respondents who had indicated their familiarity, who had had an infection on their computer and who did not know how this infection came about.

***Table 4.3**: Virus infections in relation to awareness*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Awareness	163	63.17	86	70.49	77	56.61	0.020*
Infection	128	49.61	66	54.10	62	45.59	0.173
Aware and infection	99	38.37	53	43.44	46	33.82	0.114
Unaware and infection	29	11.24	13	10.65	16	11.76	0.778
Aware and cause unknown	48	18.60	28	22.95	20	14.70	0.093

** significant at the 5% level*

Worth noting immediately is that despite an overall awareness level of greater than 60%, almost 50% of respondents had in fact suffered from a virus infection on their computers. It is also apparent that awareness of or familiarity with the term, was no barrier to infection, with more respondents who had expressed familiarity with the term admitting infections than those who had not. This could be put down to unfamiliarity with the term, although responses, though not vast in number, do indicate

that lack of familiarity with the term is not necessarily a barrier to knowing that one had been infected. With 18.60% (almost one out of every five) of 'aware' respondents admitting to infection and not knowing how their computer came to be infected, it is again shown that non-infection and knowledge of how the infection came about does not follow automatically from familiarity with the term. A Student's' t-test on the admitted infection figures gives a p-value of 0.173, which indicates that female respondents were no more likely to suffer from infection by a computer virus than their male counterparts, despite having lower levels of recognition of the term as shown in Table 4.2.

In light of the above, it is encouraging to note that despite the apparent (relative) lack of recognition or familiarity with the term 'computer virus', and the same, in terms of infections, and how they are acquired (primarily through the use of other people's USB devices was the most common cause of infection identified), was that 242 (or 93.8%) of all respondents indicated that they were aware that clicking on a harmful link could lead to a virus infection and/or theft of personal data (Question 44). The difference between male (94.26%) and female (93.38%) respondents responding positively was minimal.

It could, however, be argued that the question itself led the respondents to the correct answer. As such despite this encouraging figure, virus infection retained its status as a noted gap in the awareness levels of respondents, and owing to the prevalence of viruses, and the impact they can (and have had) on both personal computers, and in this case school networks, the importance of informing good practice around this subject cannot be overstated.

More positively purely in terms of numbers, is that 88.37% of all respondents answered that they did in fact have anti-virus software installed on their personal computers, as per Question 48. A further 8.14% of respondents answered that they did not, while the remaining respondents indicated that they did not own personal computers. While the number of respondents without anti-virus software on their machines is on the low side, it should still be considered at least a moderately significant risk, at the very least to the network to which they connect, and therefore potentially other users of the network. To further assess the risk profile of the respondents in terms of what could be

considered basic necessities of security, the responses surrounding the Windows Server Update Services (WSUS) were analysed.

***Table 4.4**: The relationship between the use of AV software and WSUS*

	Total (n=258)	%
Familiarity with the term WSUS	4	1.55
Do run automatic updates	173	67.83
AV and automatic updates	164	63.56
No AV and no automatic updates	30	11.62

The Operating Systems of the respondents' personal computers were not determined. As such while for computers running the Windows Operating Systems, the terms WSUS and automatic updates are synonymous; this is not the case for users of other Operating Systems such as Linux or MacOS. Despite this, and evidence from some of the answers provided to Question 48 indicating the use of MacOS, the assumption was made that in line with global usage figures, the majority of respondents would be using Windows Operating Systems, and hence the inclusion of the term WSUS in the list of terms in Question 36.

As WSUS is server-based, and provides a service to the client machines, rather than being installed on the client machines, this term was included to test more in-depth knowledge, for while a Windows based computer may receive automatic updates from a WSUS Server, it is not necessarily the case that the end user is aware of this and hence the term as a probe for more in-depth knowledge as noted. The term automatic updates, rather than WSUS was used in Question 49 ('Do you run automatic updates on your personal computer?') and as such any confusion around Operating Systems amongst the respondents should have been avoided.

The large discrepancy between the number of respondents familiar with the term WSUS, and those who actually ran automatic updates on their computers, could be attributed to a case of them being more familiar with the action than the term. It could be the case, for example, that in order to connect to the individual school networks,

automatic updates are configured by the school network administrators rather than the learners themselves. This would result in learners being aware of the computer receiving updates, but not necessarily of the terminology involved.

As illustrated, the majority of respondents run automatic updates, and only 4.18% fewer ran anti-virus software *and* automatic updates, which from a security point of view is the preferred option in terms of risk reduction. More importantly though from a risk perspective, 30 respondents ran neither anti-virus software nor automatic updates. Whilst anti-virus software can significantly boost a computers defences against virus infection, particularly against the method though which the majority of respondents noted as the means they were infected (USB devices), it is automatic updates that are crucial to security. These contain software and Operating System patches, hotfixes, and other updates, many of which are specifically intended to patch known vulnerabilities.

Even a small number of individuals within an organisational (such as the school) environment can pose a serious risk to the network by being vulnerable owing to being unpatched. An example of a threat to an unpatched computer is a computer worm, with which only 27.13% of all respondents indicated familiarity. Similarly, while by no means infallible, good anti-virus software can provide an effective level of protection against malware in general, which is an umbrella term which incorporates all malicious software, including spyware, trojans, worms, and viruses. The term malware itself was only recognised by 25.25% of all respondents. The second commonly recognised term was spam, which had 45.34% overall recognition. While this is not a surprising result in terms of being the second most recognised term the percentage of respondents recognising the term is surprisingly low. This is due to the global prevalence of spam emails and text messages, and that transmitted via other media. There is no statistically significant gender difference in terms of familiarity with the term.

The answers provided to Question 40 indicate that more respondents (193 or 74.8%) had received some sort of unsolicited electronic communication (via instant message, email, or text message) which could be considered spam, than had indicated that they had encountered the term (117 respondents). This is a difference of 39%. It is possible that this discrepancy arose owing to the more explanatory phrasing of Question 40: 'Have you ever received unsolicited (not addressed to you personally or specifically?).

Options were then provided for the respondents to select, including emails, instants messages (IMs) text message, the aforementioned, 'not applicable', and 'other'. In any event the result that 74.8% of respondents had received what could be regarded as spam serves to confirm the high global levels of spam proliferation.

Regarding the security threat posed by spam, 36.43% of all respondents admitted to responding in some manner to the unsolicited communication. This was despite 93.8% stating their awareness, through their answers to Question 44, that clicking on a harmful link could lead to a virus infection and/or theft of personal data. Within the results of those who responded in some manner to the unsolicited communication, 36% admitted to clicking on the link provided. An analysis of those who showed high risk behaviour by way of being aware that clicking on such a link was bad, yet also admitted to doing so shows that 12.4% of respondents fell into this category of behaviour.

While this result could be ascribed to wilful disregard of the consequences, it is worth noting that the respondents were not afforded the opportunity to state whether they become aware pre or post clicking on a harmful link. It should also be noted, in mitigation, that not all harmful links are obviously so. Nevertheless the results still indicate a level of naivety amongst the respondents regarding unsolicited contact (in the context of non-personally addressed contact, spam) and how to deal with it. An example of spam included in the list of terms is a 419 scam, in which an advance payment of some sort is typically requested of the receiver, based on a fictitious pretext. Only 3.87% of all respondents recognised the term. Notably too, many spam emails for example are attempts at information theft via phishing, itself a term recognised by only 20.15% of all respondents. Phishing attacks perpetuated through electronic spam are frequently a means of identity theft, a threat recognised by name, by only 36.82% of respondents.

Phishing is an attempt at information theft specifically through email via the use of fake websites, fake links (as mentioned above) and attempts to entice the receiver into entering credentials for the benefit of theft by a third party. Results regarding the respondent's awareness levels and practice indicate that a high proportion of them would be potentially vulnerable to such attacks. An example of a relevant attack could

be an email that purports to have been sent by one of the more popular social networking sites, requiring the receiver to click on the link provided to 'reactive their account', or enter their username and password to 'validate their account'. Without adequate awareness of such attempts at breaching their personal security of information, the vulnerability is evident.

Smishing (similar to phishing, but done via text message to mobile telephones) and vishing (automated voice based attempts at phishing), received extremely low levels of recognition by the respondents (1.93% and 2.71%, respectively). Nonetheless these pose just as significant a threat as phishing, despite being not as prevalent as the latter. With 3.10% of respondents having admitted to having entered their username and password when requested by an (impersonally addressed) email, text or voice message, and 5.43% admitting to having replied to the same, the participation numbers for engaging in these activities is low. If information security is looked at not only holistically, for the group of respondents, but also in terms of the impact on individuals within the group, then the dangers of engaging with these types of messages should be considered an area worthy of education.

The final question of the survey was '*Did you find taking part in this questionnaire has made you more aware of issues surrounding online information security and privacy?*' The response to this question was that 173 respondents or 67% answered in the negative. This response is interesting when contrasted with answers discussed above. It reinforced the notion established in this section that as a group, the respondents perceived themselves to be more aware than they actually were. Self-perception can be very inaccurate though as established, for if a respondent was aware of, for example these threats, and felt confident that they knew enough about these threats not to be at risk, then they would perhaps note in the self-perception that they were very aware. On the other hand, because the figures indicated that there are in fact many more threats out there than the respondents were aware of, it was hoped that the final question would have elicited the opposite result.

4.4 SUMMARY

In terms of the significance of the awareness levels displayed regarding the threat terms as presented above, it can be concluded that overall, the awareness levels of the respondents were lower than hoped for, and that there is a need for education not only about the terms themselves, but around the behaviours surrounding them. The largest indicator of the overall low level of knowledge, is the fact that the highest figure for familiarity with a single term is the 63.17% for computer virus, a term for which an almost 100% figure was anticipated owing to the prevalence of viruses, and the widespread notoriety of the term. Other threat terms such as browser poisoning, smishing, vishing, keystroke logging, and social engineering received very low levels of recognition. Browser poisoning was introduced not so much as a direct threat to the respondents, but as an example of a term or concept which required much deeper knowledge of threats than would be expected of the casual, or even regular computer user, even one regarded as being fairly aware. The inclusion of this term was therefore to gauge the number if any, of respondents who had this greater depth of knowledge, or at least knowledge beyond what could be considered more common terminology. Unfortunately lesser known terms do not correspond to lesser threats, and the low figures are seen as a massive informational gap, and therefore as a risk to the respondents as a group.

Knowledge of a term does not necessarily guarantee knowledge about the relevant behaviour, just as not knowing the correct term for an action does not guarantee that someone does not know the inherent risks of engaging in the action itself (or being engaged with such as in the case of a social engineering attack). Given the difficulty of detecting many of the threats, education around the existence of these threats is important in terms of mitigation, particularly in terms of awareness and behaviour modification, focused towards prevention. As such it is important to blend the use of terms and actions, so that recipients of such education would be able to understand what not to do, as well as *what it is* that they are avoiding in terms of risk.

CHAPTER 5: ONLINE PRIVACY AND SOCIAL MEDIA

This chapter analyses the behaviour of respondents regarding the usage of social media platforms and applications, and examines these patterns in terms of risk. The risks are identified in terms of threats to online privacy, as a concept, as well as resultant risks to the information security of the respondents. Whilst privacy and security are not intrinsically linked, and breaches of privacy do not necessarily constitute breaches of information security, there is a strong relationship, and this is particularly so in the online environment, and even more so within the social media context. This is due to the extensive activity within this environment, and the potential for abuse that it offers. Whilst social media forms a dominant part of this chapter, practice relating to the Internet in general is not ignored, and also features in the discussion where appropriate.

5.1 INVOLVEMENT AND PLATFORMS

Before engaging with issues relating to what content was placed on social media platforms, attitudes towards online privacy, and the behaviour of the respondents in practice, it is necessary to determine the respondents' own engagement levels with social media. As indicated in Table 4.2 (in Section 4.2), the number of respondents indicating that they had in fact encountered online privacy as a (threat) term was 47.67%. This is a disappointing result in terms of risk since, unlike some of the other terms, the words making up this term could be considered almost self-explanatory. As such this figure of less than half the respondents is possibly indicative of the remainder of respondents not only having not encountered the term, but also not having an understanding of its meaning and relevance.

Figures obtained when analysing usage patterns in Section 3.6.2 show that 74.41% of respondents spent half or more of their total Internet time engaged with social media, with 23.64% admitting to spending most of their Internet time in this manner. As noted previously, the sheer amount of time spent engaging with social media demarcates it an area of potential risk. In terms of mitigation (of some aspects) of this risk, 94.19% of respondents selected 'to maintain connections with my friends and family' as their answer to Question 22. This required them to select from four options the one that fitted best as their reason for using social media platforms and applications. Despite

this, and bearing in mind the concept that risks to information security should be considered not only in terms of group risk, but risk to the individual as well, 6.2% of respondents selected 'to meet new people' as their primary reason for social media usage.

While there are several risks in the use of social media, 'meeting new people' could be one of the more significant ones owing to the potential lack or even absence of real-life, physical meeting and or/ interaction with these people. This point is a recurring theme in both this chapter and the following one. It is because of this, that the 94.19% of respondents who selected maintenance of contact with friends and family as their reason could be considered to be at a lower risk level. Nonetheless, there are quite likely members included in this percentage who used social media platforms for other reasons, such as meeting new people too. Thus while these figures provide a snapshot of stated intent, a more accurate risk assessment needs to be determined from the behaviour exhibited.

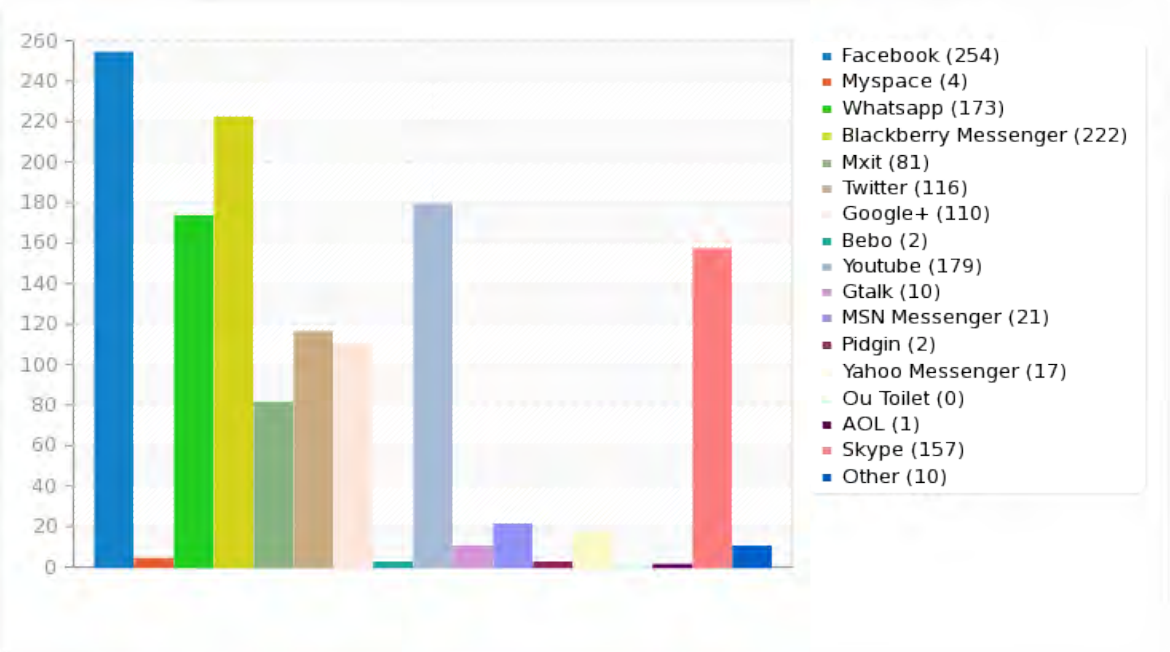

***Figure 5.1**: Usage of social media platforms as per Question 17*

Question 17 required respondents to select all of the listed social media platforms personally used by them. As shown in Figure 5.1, *Facebook*, with 98.45% use, was the most popular social media platform, enjoying significantly more use than the other web-based platforms such as *Myspace*, *Bebo*, and *Google+.* The next most popular platform was the *BlackBerry Messenger* service, for users of BlackBerry phones. This is a result

consistent with the answers to Question 13, where 87.21% of respondents listed their telephone model as being a *Blackberry*. Both of these applications provide opportunities for solicited and unsolicited contact with people who could be defined as 'strangers': people with whom little or no physical meeting time has taken place, as well as exposing users to risk of abuse as instruments for sexting and potentially resulting in cyberbullying as discussed in Chapter 6.

Of these two most commonly used platforms, *Facebook* has the greater potential for compromise of privacy and security of information. As a result, and taking into account that all but four of the total number of respondents listed themselves as users of *Facebook*, this chapter deals with it as the primary platform. It is worth noting though that other platforms that have been used as instruments of cyberbullying also showed appreciable use, notably *Youtube* (69.37%) and *Twitter* (44.96%).

5.2 VOLUNTARY ACCESS TO PERSONAL INFORMATION

This section discusses the results of analysis of the respondents' actual behaviour, and by inference their attitudes towards online interaction with people they have not met in person. By extension their allowance of such people into their online lives, and therefore access to (at least some of) their personal information, is also examined. As noted previously, with *Facebook* being utilised by almost 100% of respondents, (see Figure 5.1) in terms of web-based social media platforms, it is used as the platform discussed in terms of method of operation and overall functioning. While it was not possible to ascertain the presence, or indeed the absence of duress from the results of the questionnaire, it is presumed to be absent in terms of the sending and accepting of requests of the type discussed below. As such access granted in this manner is determined to be voluntary, although other possibilities are also examined.

5.2.1 ENGAGEMENT WITH STRANGERS

Table 5.1 summarises the answers to Questions 25 to 43. The term 'stranger' has been used to represent what was referred to in the questionnaire as 'a person you have not physically met'. As such the figures presented in this table reflect communications of an online-only nature, between the respondents and people whom they had never met in person.

***Table 5.1**: Respondents' online communication behaviour*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Communication received from stranger	144	55.81	69	56.55	75	55.14	0.820
Engaged in communication with stranger	117	45.34	64	52.45	53	38.97	0.030*
Contact was initiated by stranger	117	45.34	52	42.62	65	47.79	0.406
Contact was initiated by respondent	21	8.13	17	13.93	4	2.94	<0.001***
Stranger initiated and respondent engaged	92	35.65	45	36.88	47	34.55	0.698

** significant at the 5% level;*** significant at the 0.1% level*

The first row indicates that 55.81% of all respondents, and very similar percentages of male and female respondents, had received *personal communication* from a stranger. This type of communication differed from the impersonal communications discussed as *spam* in Chapter 4. The type of communication under discussion refers to contact made directly with the respondent, in a personal manner, for example, a message sent from a stranger to the respondent's *Facebook* account. The difference is that the respondent was contacted *directly,* rather than *generically* as would be the case with unsolicited spam-based communication of the type referred to previously.

The fact that just over half of all the respondents had received this kind of communication is indicative of the potential for information compromise and the potential risk that the unwary could fall prey to. Interestingly, of the 144 respondents who acknowledged receiving such communication, 90 or 62.5% also acknowledged *engaging in communication* with a stranger. This is a similar figure to the 92 out of 117 respondents who engaged with communication from a stranger once the stranger had initiated contact, as displayed in the last row of Table 5.1. This translates to a 78.63% rate of response to stranger initiated contact, a figure which could be considered a

indicative of the lack of awareness of the potential for harmful consequences that could result from such interaction.

Notably, as indicated by the p-value of 0.030 male respondents show a statistically significantly (at the 1% level) greater likelihood of engagement with strangers. Conversely 8.31% of respondents admitted that they had initiated contact with a stranger. While the relatively low figure is perhaps indicative of some degree of awareness surrounding the potential for risk, the actual risk remains the same. Notably too, male respondents are shown to be significantly (at the 0. 1% significance level) more likely to initiate contact with strangers. Reasons for this behaviour can be speculated upon, but were not investigated through the questions posed in the questionnaire.

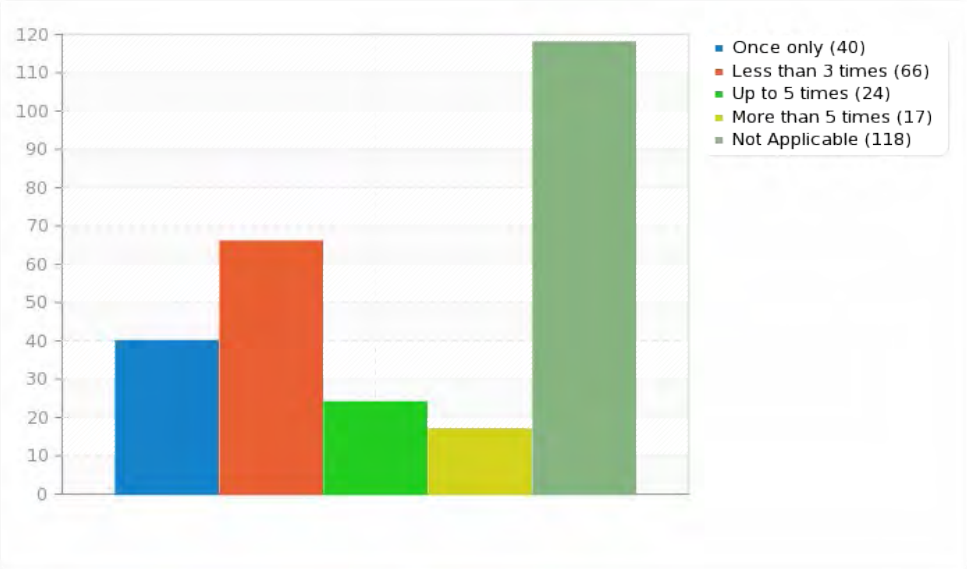

***Figure 5.2**: Frequency of engagement with strangers online*

Figure 5.2 shows that the majority of respondents who had engaged in communication with a stranger, or strangers, had done so on more than one occasion. The highest number reflected in Figure 5.2 was between one and up to three occasions. This indicates that this type of behaviour was not a series of isolated incidents, but a more consistent pattern of behaviour, though not endemic by any means. The numbers in Figure 5.2 do indicate an enhanced risk level though, for while one interaction may be potentially harmful, to engage more than once, whether with the same stranger or different ones, increases that potential for harm.

It is acknowledged that not all contact with, from, and to strangers is necessarily harmful, or takes place with mal-intent on either side. With that stated however, in terms of patterns of risky behaviour, according to the figures displayed in Table 5.1, the majority of respondents fell clearly into a category of high risk, based on their willingness to engage online with people whom they have not physically met. This willingness to engage has the potential for malicious strangers to elicit information from the respondents, which again has the potential for harm in terms of information and privacy breaches.

While the full spectrum of interaction was not examined, relevant aspects thereof are addressed in more depth as privacy concerns further on. Student's' t-test s for the significance of gender differences were run on the figures presented in this table, and as indicated, male respondents were more likely to engage with strangers, and to initiate the contact.

5.2.2 PROVISION OF INFORMATION ACCESS TO STRANGERS

Having established the respondents' basic levels of willingness to interact with online strangers through Table 5.1, Table 5.2 examines this interaction more closely in terms of allowing access to personal information to a stranger or strangers. The use of the term 'stranger' remains as previously defined. The information displayed in Table 5.2 was drawn from Questions 25 to 30.

Table 5.2: *Granting of access to information to strangers via social media platforms*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Friend request sent to stranger	93	36.04	48	39.34	45	33.08	0.298
Friend request from stranger accepted	159	61.62	79	64.75	80	58.82	0.329

Immediately apparent is the lack of statistical significance in the results: male and female respondents show no gender difference in terms of either making, or accepting 'friend' requests to, or from strangers.

The first row of this table, *friend request sent to stranger* refers to the act of sending a request to a stranger in order for them to have the requestor on their contact list, in the case of instant messages applications, or on their 'friend' list in the case of social media platforms, such as *Facebook*. In the case of an instant messaging application such as *BlackBerry Messenger*, which was identified as enjoying significant use by the respondents, adding someone to the contact list provides the means for them to communicate with the person who added them via the service. This is done through a unique-to-user, service-specific pin code, which must be shared, and does not make the actual telephone number of either participant visible to the other, unless this too is shared. With the established widespread use of both this make of cellular telephone and the messaging service, it could be stated with certainty that use of this service was a primary method of communication amongst this group of respondents.

Unlike on web-based social media platforms, there is no direct breach of personal information by adding a stranger to such an instant messaging contact list. By doing so however, lines of communication are opened, and while harassing users can be deleted or even blocked, consequences may result if other information has been shared during such communication. Whilst the discussion at this point revolves around strangers from a higher risk point of view, it is worth noting that breaches of privacy, information theft, harassment, and cyberbullying can just as easily take place amongst peers.

The implications of adding someone to a 'friend' list on a social media platform, such as *Facebook,* are greater than those on an instant messaging platform. This is due to the amount of information available to 'friends' on this platform. Once accepted as a 'friend', users have access to the personal information of the user they have become 'friends' with via that user's profile on that particular platform.

While the actual amount of data posted by users on the platform varies, the categories of data available for posting, and therefore viewing, include photographs and other personal details including date of birth, location, school, employer, email address, telephone number, lists of other contacts, profile posts by other 'friends' or contacts, and posts by the profile owners themselves. As discussed in Section 5.3, there are measures that can be taken to adjust privacy settings, but essentially once a person has been accepted onto a 'friend' list, they have access to the majority of information posted

in the profile, unless specific measures have been taken against this, and even then some information is still available.

Returning to Table 5.2, the first row showing figures for *friend request sent to stranger* reveals that 36.04% of all respondents had actually sent a request to a stranger. The question did not differentiate between a web-based platform such as *Facebook* as described above, and an instant message application. Also, as discussed above the implications are slightly different, but in privacy and security of personal information terms, the concept is the same: inviting someone who has never been physically met or even seen and who is therefore essentially an unknown quantity in all respects, into one's life. In terms of risk, a case could be made for stating that the same level of risk would apply in such a scenario as it would in the case of engaging with strangers in person outside of an online environment: not every stranger is dangerous, but the potential is always there. As it is a societal norm to encourage young adults within the age range of these respondents to be wary of personal interactions with people they do not know (in some circumstances), so too similar rules (should) apply to online behaviour in terms of risk, perhaps even more so, as the risk is not always as apparent online.

The major difference then, is that while a physical assessment can be made of people when meeting them, when interacting with strangers online there is no way of establishing if they are who and what they say there are, in terms of age, appearance, gender, occupation, or any of many other characteristics. That 36.04% of respondents indicated that they had essentially invited unknown quantities into their lives is a concerning figure. This is again based on taking into account risk to the individual as well as to the collective. Reasons for this proactive behaviour on the part of the respondents were not established, however, analysis shows that of the 92 respondents who had engaged with a stranger after *contact was initiated by the stranger* as per the *stranger initiated and respondent engaged* row in Table 5.1, 45 of them (48.91%) had also sent a friend request to a stranger (in contrast to the overall figure for this behaviour of 36.04%, shown in Table 5.2, which included those who had not done so after the stranger initiated contact).

Conclusions that can be drawn from this figure include that once the contact had been established by the stranger, and lines of communication opened, the respondents had been coerced or manipulated into a relationship of some sort, which led the respondent to send the request. Perhaps just as possible however, is the likelihood that there was no manipulation or coercion and that the respondents were either simply curious, or had established a *bona fide* relationship post-contact. Should the first of the two possibilities have been the case, then it is worth noting at this point the potential for harm caused by the social engineer.

It is shown in Table 4.2 (in Chapter 4) that only 13.56% or 35 respondents out of the 258 claimed to have encountered the term social engineering. As noted previously in Chapter 4 the term has usage outside of the information security context, and as such respondents may have encountered the term elsewhere, affecting the answers to this question. Social engineering can be defined in several ways, as it is in Chapter 2. One of the most common and relevant in this context is "getting people to do things they wouldn't ordinarily do for a stranger." (Mitnick and Simon (2002:xi). An immediate example of this relating to Table 5.2 is the 48.91% of respondents who have themselves invited strangers into their online lives following contact with strangers (and to a large extent therefore their real lives as well).

The above is not intended to draw the conclusion that the entire 48.91% were tricked by social engineers into inviting them into their lives, but to illustrate that it *could* have been the case, in some, or even all of the instances. Conversely, the row in Table 5.2 titled *friend request from stranger accepted* shows that 61.62% of respondents accepted strangers into their online lives (with varying degrees of access, depending on the platform, as discussed above), at the behest of the stranger. This poses similar dangers if it happened the other way around (the respondent making the request to the stranger rather than receiving it) as discussed, but the implication in this instance was that the driving force behind the communication and ultimately the requests were the *strangers*, rather than the respondents. That said, many of these accepted requests could have been the result of requests only, i.e. without preamble. In this case a friend request from a stranger would be received and simply accepted on the basis of a profile picture for example, without any actual 'work' by the stranger.

To confirm this, an analysis was performed on those respondents who had accepted a friend request from a stranger *and* who had indicated that they had not engaged in communication with a stranger. The result shows that 59 respondents (this was taken from respondents who had answered 'no' to engagement with strangers and who had accepted a friend request from a stranger) out of the 159 (37.10%) who had accepted friend requests from strangers had done so without any prior communication taking place and therefore without coercion, manipulation, genuine established communication or any other readily discernible (from this survey) reason.

The dangers of this have been discussed, but it is worth noting that in both instances, the respondent had the option to either send the request, or refuse to accept it. While this pattern of behaviour holds risk, like most online threats, it is quite possible to avoid the risk successfully. As analogous example, a user may successfully avoid a virus infection by not clicking on attachments in emails which arrive from people they do not know. Despite this, interpersonal interaction (even online) can be more complicated than purely electronic threats such as viruses. Problems (within the scope of this research, and in the context of online privacy and information security) arising from interpersonal interaction are also potentially less easy to eradicate than the aforementioned example of a virus infection, as illustrated in Chapter 6.

The figure of 37.10% referred to above, shows that more than a third of respondents had admitted accepting the friend request of a person they had not met in an offline situation, and by virtue of the established lack of communication, a person with whom the only contact they had had was the actual request received. In terms of potential education, this is an area that clearly needs some focus, based on the potentially risky behaviour displayed by the respondents. Interestingly, in terms of this risk, 83 respondents (32.17%), or almost a third of all respondents, had both sent a request to a stranger and accepted a request from one.

Based on the way that social media platforms work, in that a request from one party, once accepted results in both parties appearing on each other's list, network, or platform (there is no need for a reciprocal request, just acceptance from either party), these respondents were engaging in the highest risk level of all the respondents in this

context. Privacy breaches, information theft, sexting, cyberbullying, and social engineering, are all intrinsically linked as threats.

Returning to the threat of social engineering, in the context of the above, "…to manipulate people, by deception, into giving out information, or performing an action" is a highly appropriate definition provided by Mann (2008:11). An example of this in the light of the current discussion would be the manipulation of someone into accepting a friend request, or even extending such a request, with the aim of gaining access to their personal information. Another definition, appropriate here through the use of the word 'target' is Hadnagy's (2010:10) view that "…a true definition of social engineering is the act of manipulating a person to take an action that may or may not be in the 'target's' best interest. This may include obtaining information, gaining access, or getting the target to take certain action."

A key point worth considering from this definition within the current discussion surrounding engagement with online strangers is the phrase '*may or may not be in the target's best interest'*. This phrase sums up the underlying problem, and potential for harm which is inherent to the risky activity of engaging online with people who are actually unknown in any capacity. Both of these definitions show direct relevance to the issues of communicating with a stranger, and inviting or accepting a stranger into one's online life as discussed.

Reference was made earlier to the fact that strangers may not be who they appear to be, or present themselves as, in terms of appearance, gender, interests, school, location, etc. There is a stereotypical example of where a social engineer, in reality a 50 year man could present himself as, for instance a 15 year old girl, and attempt to befriend and gain access to the information of boys of similar age, for any of many purposes, none of them to the benefit of the targeted boy, as per the selected phrase from the definition provided by Hadnagy (2010) above. It is for this very reason that an educational emphasis should be placed on the dangers of interacting online with strangers.

***Table 5.3**: Sending and acceptance of stranger contact requests by age and gender*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Request accepted (stranger within 5 years older)	104	40.31	51	41.80	53	38.97	0.645
Request sent (stranger not within 5 years of age)	21	8.13	9	7.37	12	8.82	0.671
Request Accepted (stranger not within 5 years of age)	25	9.69	15	12.30	10	7.35	0.187
Stranger was the opposite gender (Request accepted)	104	40.31	57	46.72	47	34.55	0.090
Stranger was the same gender (Request accepted)	52	20.15	21	17.21	31	22.79	0.090
Stranger was the opposite gender (Request Sent)	66	25.58	34.00	27.87	32.00	23.53	0.315
Stranger was the same gender (Request Sent)	41	15.89	17.00	13.93	24.00	17.65	0.315

Examining Table 5.3, where the sending and acceptance of requests is broken down further by categories of age and gender of the stranger, it is clear that in the majority of cases where respondents had accepted a 'friend' request from a stranger, this person was older than the respondent, but within five years of their age. Whilst this constituted 40.31% of the total number of respondents, more tellingly, it also constituted 65.40% of respondents who had accepted a 'friend' request from a stranger.

Taking into account the ages of the respondents, this translates to a 15 year old respondent accepting a request from a 20 year old stranger at the lower level, or an 18 year old respondent accepting a request from a 23 year old respondent. The five year

age range was selected as it would not be unusual for a learner in Grade 8, of approximately 14 years of age to have contacts or friends on their lists who were in Grade 12, and ordinarily around 18 year old as an example. While age in itself is not an indicator of risk, it was decided that for the purpose of risk assessment via the questionnaire, five years would provide a 'safer' range for interaction on social media platforms.

To assess higher risk levels the category of 'Not within 5 years' was introduced. In this category, split between requests sent, and those received and accepted, a total of 17.82% of respondents fall into the broad category of having sent (8.13%) requests to or accepted (9.69%) requests from strangers who were not within five years of their age. As stated, age is not an absolute indicator of risk level, and so, based on age, risk is determined as potential risk, with the actual harm in terms of information compromise and resultant consequences stemming from the behaviour exhibited post acceptance of the request, which should be seen as a 'gateway' into the respondent's information and lives. Nonetheless, considering the age range of the respondents, a gap of over five years, for interaction with a stranger, either older or younger could put the respondent at an increased risk.

As an example if a 16 year old male respondent were interacting with a 10 year old stranger, there could be legal ramifications for that respondent, depending on what transpired. Similarly, if a 16 year old female respondent were interacting with a 25 year old stranger, while there may not be legal ramifications, there may be others, considering the age gap *and* the fact that the respondent would still be at school compared to a 25 year old working person.

It must be emphasised that not all interactions with strangers, including regarding 'friend' requests are necessarily harmful, and that not all age differences of over five years need be devoid of innocence. Nonetheless the risk potential should be clear, and the evidence available from these respondents is indicative of high risk to individuals, though the risk is lower when the respondents are considered as a group, from the perspective of interaction in age terms. Not unexpectedly, in the majority of cases where a stranger's 'friend' request had been accepted, 65.40% of these strangers were of, or represented themselves as being of, the opposite gender to that of the respondent who

had accepted the request. Additionally, 70.96% of respondents who had sent a 'friend' request to a stranger, had sent one to a stranger of, or representing themselves to have been of the opposite gender to the requestor.

This is not unexpected, for two reasons, the first one being that it is conceivably natural to be curious about and want to meet and interact with attractive looking individuals of the opposite gender. The implication of this is that perhaps the respondents had come across an attractive picture on a profile, possibly with some personal information visible, and decided to attempt to establish contact. The second reason is that following communication from such a profile, the respondents were enchanted enough to make the 'friend' request.

It is worth reiterating that 48.91% of respondents who received communication from a stranger had gone on to send a friend request to a stranger, although it was not determined whether the requests were sent to the same strangers that had initially contacted the relevant respondents. Statistically, there is nothing to indicate in Table 5.3 that male or female respondents were more or less likely to have exhibited different behaviour, based on their gender.

5.2.3 INFORMATION DIVULGED TO STRANGERS

Perhaps the most damning indictment of the behaviour of the respondents in terms of privacy and risk illustrated thus far is the data given in Table 5.4. This reveals in more detail through the different categories displayed, the types of information the respondents had provided to someone who they had not physically met, that as per answers to Question 35. As a concept, divulging personal information to strangers, in the context of the term as it is being used, is classified as high risk behaviour in the contexts of both online privacy and information security, as discussed throughout this chapter. More specifically the information revealed to have been provided to strangers could be considered to be exactly the kind of information that a social engineer would seek to elicit for any of a number of purposes, none of which would likely be of benefit to the provider of the information.

Table 5.4: *Divulging of personal information to strangers*

Information Divulged	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%
Name of your school	70	27.13	39	31.97	31	28.68
Your Location	29	11.24	13	10.66	16	11.76
Any details of your family	12	4.65	8	6.56	4	2.94
Any details of your friends	15	5.81	9	7.38	6	4.41
Financial details	3	1.16	3	2.46	0	0.00
Your phone number (home, hostel, or cell)	26	10.08	17	13.93	9	6.62
Your email address	24	9.30	14	11.48	10	7.35
Not applicable	150	58.14	67	54.92	83	61.03
Other (open ended option)	20	7.75	n/a	n/a	n/a	n/a

It is also worth noting that while this information was provided by the respondents, and considering the phrasing of Question 35, was presumed to be done so freely, there remains the possibility that there may or may not have been elements of duress involved. There is however, no basis for confirmation of this through the research conducted, and as such the answers provided by the respondents were regarded under the aforementioned assumption.

Considering Table 5.4, in the bottom row which denotes responses given as 'Other?' these responses were provided as qualitative answers, and the majority (of the small percentage that selected this option) did not specify any actual information. Of those who did, two answers stuck out. These are 'it was my exchange' (meaning an exchange student) and 'it was my cousin' (whom presumably had never been met). Both of these cases, although not actually answering the question asked, are examples of where online interaction with strangers could have a genuine, (relatively) low risk reason for occurring. This serves to emphasise the earlier point made that not all interaction with strangers is necessarily harmful, but that as a concept it should be regarded as risky behaviour.

Returning to Table 5.4, the two categories of information that are immediately noteworthy are the making available of telephone numbers and financial details. The latter was a tiny percentage of the overall sample group, and although the specifics of the details handed out (for example banking details / credentials or details of the respondents' own or family's financial situation) were not determined, the concept of handing over financial details to an unknown should be classified as very high risk. This is because there are very few, if any, scenarios where a stranger would need (or indeed want) financial details from someone they have not met without a nefarious purpose in mind.

Regarding telephone number(s), this category included any, or all of home, boarding house or personal cellphone numbers, none of which are easily changed, especially by a respondent within the school environment and within the age range of the sample group. Bearing this in mind, a compromised telephone number could potentially lead to unwanted and/or unpleasant communication or interaction, perhaps escalating to harassment, with there being a limit to what the victim in this case would be able to do in terms of corrective action.

While almost the same percentage of respondents indicated that they had given away their email addresses (9.30% compared to the 10.08% who gave away their telephone contact details), it is easier to block someone who is providing unwanted attention via email, or even on a social media platform, such as *Facebook,* or any of the instant messaging applications such as *BlackBerry Messenger* than it is via telephone. This is especially true if a landline, and a communal one at that, is involved, as would be the case in a boarding house at any of the schools surveyed. This becomes more complicated potentially if the name of the school has been provided to the stranger as was the case with 27.13% of all respondents, making it the most commonly given out category of personal information. With the name of the school known, it would not necessarily be difficult using the social engineering techniques of *pretexting* and *elicitation*, as well as *footprinting*, which was defined by McCreevy (2002) as the gathering of publically available data, to gather enough information to work out or acquire email addresses or telephone numbers. Pretexting is defined as "…the act of creating an invented scenario to persuade a targeted victim to release information or perform some action." This scenario generally also involves the social engineer in

"…impersonating people in certain jobs and roles that they never themselves have done" whilst often in doing so having to "…create a whole new identity and then using that identity to manipulate the receipt of information" (Hadnagy 2010:78). Elicitation is the extraction of information from people by drawing it out of them, through conversational means (Hadnagy 2010).

Details of family and friends provide further information to receiver of this information about the provider, and the more information that is available about someone the easier it becomes to make use of pretexting and elicitation as mentioned above. These details remained unspecified but could have included names, addresses, contact details, or any other personal information. Location was the second most commonly provided piece of information, with 11.24% of respondents admitting to imparting this information to a stranger. Retrospectively this part of the question was ambiguous, for 'your location' could have been taken to mean 'your location at some point' as in, where a respondent was at a particular time when interacting with the stranger, or it could have meant 'your location' as in a permanent or semi-permanent one such as a home or boarding house, rather than a transient/current location. Location in this instance could have been taken to mean geographical location as in town or city. In any of the instances above, providing a location at best allowed access to knowledge of where the respondent lived, in a semi-secure boarding school or home environment and at worst provided on-the-spot information to a potentially malicious stranger of where the respondent was at a particular moment.

No statistically significant gender differences in behaviour and therefore risk level were determined from the information in Table 5.3. This is again consistent with the rest of the information presented in this section, with the exception of the male respondents' communication with strangers as discussed. While the figures for information provided to strangers in Table 5.4 are not high numerically, there are sufficient respondents to indicate a high level of risk based on the behaviour exhibited, a finding that is again consistent with the results of this section.

5.3 PRIVACY IN PRACTICE

In this section awareness and practice surrounding the concept of online privacy are discussed along with respondents' actions to enhance their privacy. Answers to questions on privacy as a concept are analysed, as are answers to questions relating to actual steps taken by the respondents to enhance or ensure the privacy of their personal information. As noted previously, security of information and the privacy thereof can be strongly linked, as has been the trend in this chapter. While there was a strong emphasis on interactions with strangers previously, and while that thread is continued to an extent, there is also a focus on peers and on privacy in general. Discussion regarding the relevance of the social engineer as a threat to the aforementioned is continued from the preceding sections where appropriate. Information discussed in this section also has broader relevance to other chapters, specifically Chapter 6, dealing with sexting and cyberbullying. While the previous section dealt with voluntary or deliberate parting with personal information, this section looks at parting with information from a more inadvertent than deliberate perspective.

5.3.1 INFORMATION MADE AVAILABLE ONLINE

Question 45 required the respondents to indicate what material they placed online, by selecting those applicable from a choice of three options. The results fall well within what may be considered the normal range of usage of social media platforms, considering the very nature of social media: pictures (86.05%), text and comments (80.62%), and videos (15.89%). As a follow-up, Question 46 required respondents to answer if they had ever placed anything online which they would not like their parents to see. From the answers to this question, 22.47% of respondents indicated that they had done so, although the exact nature of the material was not investigated. This question was posed to gain insight into the respondents sense of privacy, considering that if material was not considered appropriate viewing for parents, it may not have been appropriate viewing for anyone else either. This figure could be taken as an indicator that respondents were at least to an extent, cognisant of the concept of keeping some things private.

Interestingly, 39 or 15.11% of all respondents admitted to placing something online which they would not have liked their parents to see *and* had participated in the activity

of sexting (see Table 6.1 in Chapter 6). However, with the total number of respondents who had participated in sexting numbering 61, these 39 respondents mentioned above totalled 63.93% of those involved in sexting, which shows a link between the two actions. This is also an illustration that while these respondents were aware that their actions in these instances were perhaps not in their best interest, they went ahead with them anyway.

As a follow-up to this, responses were obtained indicating that 32.95% of all respondents had placed information or photographs online under the belief that it was private, and then later discovered that this was not the case. This points towards the respondents' ignorance or naivety towards the privacy or otherwise of material posted online. This in turn opened the door to further investigation of this concept, beginning with the awareness and use, or lack thereof, of the adjustable privacy settings available to the respondents.

5.3.2 AWARENESS AND UNDERSTANDING OF PRIVACY POLICES

Table 5.5 is constructed from the answers to Questions 60 and 61, which sought to gauge the awareness and understanding of online privacy policies for the social media platforms used.

***Table 5.5**: Awareness and understanding of social media privacy policies*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Privacy policies read on any Social Media platform	156	60.47	62	50.82	94	69.12	0.002**
Read and understood	90	34.88	37	30.33	53	38.97	0.145
Read but uncertain	66	25.58	25	20.49	41	30.15	0.074
Not read	104	40.31	61	50.00	43	31.62	0.002**
Awareness of *Facebook* privacy settings	214	82.95	93	76.23	121	88.97	0.033*

** significant at the 5% level;** significant at the 1% level*

Evident from this table, is that the majority of respondents had at least read a privacy policy on one or more of the social media platforms used by them, with 60.47% having done so. This figure dropped by almost half though to 34.88% when the rider 'read and

understood' was added as a filter. This, in addition to the 40.31% of respondents not having even read the policies, is indicative of two things. The first is that based on the latter figure, a large number of respondents were either not aware, or worse, were aware but did not bother to read the policies. The second is that even though the majority of respondents had read the privacy policy on at least one of the social media platforms in use by them, the overall level of admitted understanding was relatively low. This evidenced is further strengthened by the 25.58% of all respondents, or 42.03% of those who had read at least one privacy policy having admitted that they were uncertain about the contents or meaning of what they had read. An outcome of this information is that respondents require education in terms of being aware of the existence of privacy policies and the importance of reading them but *also* education regarding their *meaning* and *implications*. This is a point worth noting for incorporation into possible future attempts at addressing this issue though relevant education.

The final row in Table 5.5 reflects the number of respondents who indicated that they were aware of the privacy settings available to them on *Facebook*, the most used social media platform, enjoying 98.44% usage amongst the respondents. It should be noted that this question was phrased to ensure that the awareness of the settings *available* to the users was the question being answered, rather than simply being aware that there are settings. By implication, knowing which settings are *available* means awareness of the actual settings, rather than simply the concept that the site in question has adjustable privacy settings.

When considering the relatively high figure of 82.95% who acknowledged being aware of these privacy settings, compared to the 60.47% who had read at least one policy, it showed that a considerable number of respondents were aware of the availability of settings, but did not relate them to policies, perhaps viewing the two as separate entities, rather than being intrinsically linked. This too is an aspect of privacy that needs addressing amongst this group of respondents, as it reveals a lack of deeper understanding of the privacy concept.

Tests for statistically significant differences between the answers provided by the different genders were conducted via Student's' t-test s. While most figures displayed in

Table 5.5 lean towards showing that female respondents were superior (in terms of positive behaviour exhibited) in all of the categories, the statistical tests indicate that in terms of significance, this is the case, but in only three out of the five categories: privacy policies read on any social media platform (significant at the 1% confidence level) and awareness of *Facebook* privacy settings (significant at the 5% confidence level). In each of these categories female respondents were more likely to have read any privacy policies, and more likely to be aware of *Facebook* related privacy settings. Male respondents are shown to have been statistically less likely (at the 1% level) than their female counterparts to have read a privacy policy. Based purely on these figures, it was possible to conclude that female respondents had an advantage in terms of personal responsibility for their online privacy, in terms of *awareness and understanding of social media privacy policies.*

While the adjustment of settings can increase aspects of online privacy, there is more to ensuring privacy than adjusting settings. This is why the policies, and the reading and understanding thereof are important: they can make the user aware of what information is private, as well what can be adjusted to be made private and what cannot, and therefore the limitation of the privacy controls available. This information can provide the user with a more informed picture of their information in privacy terms, and allow for better decision making and choices regarding not only information placed on a platform, but even which platform(s) to use and which to avoid. As an example, it would be of limited value to a user in online privacy terms to make photographs posted on a web-based platform 'private' to other site users via the native privacy settings of the platform, only for the company running the site to allow, in terms of its privacy policy all of those images to appear in a simple search engine image search.

5.3.3 PRIVACY SETTINGS AND SOCIAL MEDIA

Having differentiated between policies and settings, and established some levels of awareness and understanding around these areas, Table 5.6 assesses the level of effort made to adjust settings. The information in this table is drawn from the answers Questions 50, 52, 53, 56, 62 and 63. Immediately apparent from the figures presented, is the discrepancy between the numbers in the 'total' column for the first three rows. In

the second row, 81.78% of respondents indicated that they were aware of how to adjust privacy settings on social networking platforms. Yet when responding to whether they had in fact changed any of these settings, the figure dropped to 69.38%. This may be explainable in the same manner as previously; i.e. that awareness does not translate into action, owing to lack of concern or interest, ignorance regarding the concept of privacy, or for other unexplained reasons.

Table 5.6: *Adjustment of privacy settings by respondents*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Steps taken to improve privacy	125	48.45	50	40.98	75	55.15	0.022*
Aware of how to adjust social media privacy settings	211	81.78	96	78.69	115	84.56	0.227
Privacy settings changed (social media)	179	69.38	80	65.57	99	72.79	0.212
Privacy settings changed on phone	153	59.30	70	57.38	83	61.03	0.553
Privacy settings adjusted on web browser	141	54.65	68	55.74	73	53.68	0.741
Allow location via cellphone	91	35.27	51	41.80	40	29.41	0.021*

** significant at the 5% level*

When the respondents were asked if they had ever taken steps to improve their online privacy, the numbers dropped further, to 48.45%. This may be rationalised in the same way as the previous in comparison the 81.78% indicating awareness of the settings. Nevertheless this figure is in contrast, or even conflict with the 69.38% who had indicated that they had changed settings. The 48.45% stems from Question 56 ('Have you ever taken any deliberate steps to improve your online privacy?'), which followed the questions from which the previous responses were elicited, and as such a different result was expected, considering the results of the previous two questions. The only explanations that can be offered without more information available for the differential between the results, is that confusion may have arisen, stemming from one question

referring to steps taken on social media platforms, and the other referring to online privacy in general terms.

Nevertheless, respondent numbers for both rows in which it was indicated that adjustments had been made, remained significantly below the 81.78% who indicated their awareness of settings, at least in terms of social media platforms. Whilst the reasons for this were speculated on previously, further research would need to be conducted in order to get a more definitive answer. What remains in no doubt however, is that awareness of settings does not guarantee corrective action, in the same way that having read a privacy policy does not guarantee either action or an understanding of the implications of that policy.

Interestingly, of the 211 respondents who indicated their awareness of how to adjust their social media privacy settings, 134 of them had *also* read the privacy policy of at least one social media platform, and either understood it, or read it and were uncertain as to their understanding thereof. This translates to 63.50% of those who were aware of how to adjust the relevant settings, indicating some degree of correlation between being interested enough to read privacy policies and adjust the settings, and vice versa, meaning there is a link between interest/awareness, and action. The fact that more respondents were aware of how to adjust settings than were inclined to read policies is perhaps indicative of taking personal responsibility on the one hand, but not realising the full implications on the other.

A total of 54.65% of respondents indicated that they had made an adjustment to the privacy settings on a web browser, which perhaps indicates a more advanced knowledge of privacy both as a concept and technically, than the previous figures suggest. Examining the number of respondents who had changed a privacy setting on their phone, compared with the number who indicated in row 2 of Table 5.4 that they had changed privacy settings for social media platforms without specifying on which device, it is apparent that of the 179 respondents who had done the latter, 68.71% had also indicated that they had changed privacy settings on their phones. This could be indicative of the strong link between social media use and the use of phones to access such platforms.

The final row in Table 5.6 represents results drawn from the answers given to Question 62: 'Do you allow your cellphone to advertise your location when you go somewhere, via *Facebook* for example?' The answers from the options 'yes' and 'sometimes' were combined to give a broader picture of the attitude towards and practice of location sharing, providing the total of 35.27%. The dangers of advertising one's location were discussed in the previous section, and it should be noted that location sharing on some makes of cellphone, such as the Blackberry, which was shown to enjoy high popularity amongst the respondents is turned on by default, therefore requiring deliberate action on the part of the user to disable it. How well this fact was known by those who answered 'no' to this question was not determined, and as a result, through possible ignorance more respondents were potentially doing this than admitted so.

Examining Table 5.6 for differences between the answers given in terms of the genders of the participants, it is shown that female respondents are more likely to have adjusted privacy settings, a difference statistically significant at the 5% level. This is consistent with the results for female respondents in Table 5.5, showing that females are more likely to have read privacy policies, more likely to be aware of the settings available for adjustment on *Facebook*, and also more likely to have adjusted any privacy settings. It is also shown in Table 5.6, that female respondents were less likely to allow their cellphone to advertise their location. With a p-value of 0.021 this is statistically significant at the 5% level.

These figures are consistent with those in Table 5.5 and indicate a better attitude towards privacy both in terms of awareness and general practice amongst female respondents, and therefore a reduced level of risk from privacy breaches than their fellow respondents of the opposite gender. Reasons for this were not established, but it is possible that this is due to the attention given regarding the dangers of the Internet in terms of privacy and 'stranger danger', and certainly much of the press coverage (see Appendix A) has been focussed on the negative impact on females, thus making them more cognisant of their potential vulnerability. In light of the figures above, it is worth noting that despite only 47.67% of respondents having indicated that they had encountered the term online privacy (see Table 4.2) many of the figures on display in the tables in this section indicate higher overall percentages than that. This is likely due

to an initial unfamiliarity with the term being replaced by a greater understanding as the subsequent questions asked provided greater insight.

5.3.4 INFORMATION PRIVACY ON *FACEBOOK*

With the previously established widespread use amongst the respondents of *Facebook* as a social media platform, and in order to drill deeper into their use of these platforms, Table 5.7 shows the information that was made available by the respondents on their *Facebook* profiles. There is no need to evaluate gender differences or examine the information in this table too closely in terms of privacy, for by publishing this information on their *Facebook* profiles the respondents were using social media as it was intended: an online representation of themselves or their personalities, through which they could connect to other people. With that stated however, the expectation implicit to the publishing of details such as telephone numbers, *Blackberry Messaging* PINs and other contact details, even if visible only to be people on their 'friend' list, is that people should make use of them.

Table 5.7: *Information available on respondents' Facebook profiles*

	Total (n=258)	%
Name Of Your School	222	86.05
Date of Birth	235	91.09
Age	209	81.01
Cellphone number	88	34.11
Relationship Status	129	50.00
Blackberry Messaging PIN	128	49.61
Home Telephone Number	20	7.75
Boarding House Telephone Number	7	2.71
Instant Messaging Contact Details	44	17.05
Postal Address	14	5.43
Home Address	34	13.18
School Email Address	58	22.48
Personal / Private Email Address	75	29.07
Your Location	99	38.37
Activities and Interests	160	62.02

At this point, as established, it is worth reiterating that not everyone on the respondents' *Facebook* 'friend' lists is necessarily an actual friend, or even personally known to the respondents. While Table 5.4 showed similar information, but in the context of having been actively provided to a stranger, the information displayed in Table 5.7 simply reveals the information that respondents placed on their profiles. It could be argued that placing no information would negate the purpose of social media applications, especially from a social networking perspective. As such the issue then, regarding privacy, is not so much *what* is placed on the profile but *who* is able to see it. Table 5.7 provides the background to Table 5.8, which in turn shows *what* information is available to *whom* on the *Facebook* profiles of the respondents.

Table 5.8 is constructed from information drawn from the answers to Question 59. Respondents were provided with a list of categories of information, almost identical in makeup to that in Table 5.7, and asked to indicate whether that information was (to the best of their knowledge) available to be viewed by 'friends only', friends of friends' (this is a setting on *Facebook* that allows certain information to be available to, as the name implies, 'friends' of the respondents' own 'friends', but who are themselves not on the respondents' 'friend list'), and 'everyone'. 'Friends only' refers to people who have been accepted onto the 'friend' list of the respondent, through the process of requesting and acceptance as detailed previously. 'Everyone' refers to the information being visible publically, that is, to people who have no connection established with the respondent.

This allows all site users to see this information without having to meet one of the previous criteria of being 'friends' or a 'friend of a 'friend'. This is clearly the lowest level of privacy, although the 'friend of a friend' category has high risk levels too: there is little difference between someone who is on the 'friend' list of someone they barely know, and through this has access to personal information of the respondent, and a complete stranger, in terms of risk and unnecessary (and perhaps unwanted) access to personal information. All figures in Table 5.8 are given as percentages.

***Table 5.8**: Access to information on the respondents' Facebook profile by category(%)*

	Friends Only			Friends of Friends			Everyone			Unsure / No answer		
	Total	M	F	Total	M	F	Total	M	F	Total	M	F
Name Of school	40.70	31.97	48.53	14.34	10.66	17.65	24.81	35.25	15.44	20.16	22.13	18.38
Date of birth	47.29	35.25	58.09	13.95	12.30	15.44	22.87	32.79	13.97	15.50	18.85	12.50
Age	44.57	34.43	53.68	14.34	14.75	13.97	20.54	31.97	10.29	20.83	19.46	22.06
Cellphone number	36.82	36.89	36.76	6.59	6.56	6.62	4.26	7.38	1.47	51.94	48.36	55.15
Relationship status	35.66	27.87	42.65	8.53	8.20	8.82	14.34	20.49	8.82	40.70	41.80	39.71
Blackberry Messaging PIN	40.70	40.98	40.44	7.36	6.56	8.09	9.30	16.39	2.94	43.02	36.89	48.53
Home telephone number	17.05	17.21	16.91	3.49	3.28	3.68	2.71	4.92	0.74	76.74	74.59	78.68
Boarding house telephone number	12.02	10.66	13.24	3.88	3.28	4.41	1.94	3.28	0.74	81.40	81.15	81.62
Instant messaging contact details	24.81	23.77	25.74	5.81	4.92	6.62	4.26	7.38	1.47	65.89	65.57	66.18
Postal address	15.12	13.11	16.91	2.33	2.46	2.21	1.94	3.28	0.74	80.23	80.33	80.15
School email address	22.09	18.85	25.00	4.26	6.56	2.21	3.49	6.56	0.74	71.71	71.31	72.06
Personal / private email address	25.58	22.13	28.68	6.20	8.20	4.41	6.20	9.02	3.68	61.24	59.02	63.24
Respondent location	31.40	27.87	34.56	7.75	7.38	8.09	9.69	12.30	7.35	50.78	51.64	50.00
Activities and interests	39.92	32.79	46.32	9.69	9.02	10.29	14.34	21.31	8.09	34.11	32.79	35.29

Theoretically the 'friends only' category would be the most secure in terms of personal information. This is dependent on who the owner of the profile invites (and the invitation being accepted) and whose invitation they accept, giving them control over this. It was shown earlier however that within this group of respondents there was a substantial number who both invited and/or accepted invitations from people they had not met, thus negating to an extent the power they had over their information. Nevertheless, there are still options on *Facebook* to control what information is visible to whom though; it is not an all-or-nothing choice. In light of the 82.95% of respondents who were aware of these options as shown in Table 5.5, these choices were further examined.

It is acknowledged that not all of the participants would have had a full understanding of what this question required of them, and this is evidenced though the previous result that some 17.05% of respondents were not aware of *Facebook* privacy settings. To assist respondents, the terminology used was specific to *Facebook*. The answers provided which stated 'I am not sure' or which were left blank, were combined to provide the number in the last column.

The most striking aspect of this table, in light of the previous paragraph, is that the highest percentage for a category of information being set to 'friends only' is 47.29%. While this, and all of the other figures in the 'friends' only column could be considered low, when viewed in the context of the previous figures for privacy awareness and actions, such as the 48.45% of all respondents who had taken steps to improve their o*nline privacy*, and the 34.88% of all respondents who had both read *and* understood a privacy policy, there was an element of consistency. More encouragingly there are no figures in the 'friends of friends or 'everybody' columns that exceed those in the 'friends only' column. This indicates that although as an overall behaviour pattern the adjustment of settings to enhance privacy is on the low side, that there is still some knowledge backed up by action, and that personal information should be protected. On this platform, this is best done by restricting information to at the least 'friends only', at the very least, although the definition of 'friend' as has been shown, appeared to be flexible at best, and meaningless at worst.

The majority of percentages in the 'friends of friend's and 'everybody' columns are single figures, which while emphasising the above also serves to lower the potential risk to the *overall group* rather than to the individual (s) in terms of the aforementioned social engineering attacks. The categories of information listed in Table 5.8 would be of use to anyone attempting to perform the actions of a social engineer, and win the confidence of or gain further access to a profile owner, for any of a number of reasons, not necessarily any of them of benefit to the 'target' as previously determined. Also as previously noted, the more information available about a 'target' the easier the task of the deliberate social engineer and other more casual or less organised malicious parties. Thus the importance of this table in illustrating the actual privacy levels of the respondents' personal information on the social media platform most commonly used by the sample group.

Table 5.9 displays similar information to Table 5.8, but the data was analysed by gender to determine statistical significance of the differences. In a qualified sense the 'most private' and 'least private' categories were analysed in this fashion. These were 'friends only' and 'everyone', respectively. Analysis was performed on these two categories in order to ascertain any gender based differences in the protection of personal information via privacy settings on the *Facebook* platform, based on the upper and lower options available, rather than an all-inclusive investigation of all four of the available categories. As per Table 5.8 all figures in this table are given as percentages bar the p-values.

When examining the p-values for the 'friends only' category, a familiar pattern appears: while there is not an abundance of statistically significant differences between the genders (5 out of the 14 categories), those that are statistically significant are in favour of female respondents. This confirms the trend shown in earlier analysis in this section, that female respondents were more likely to take steps to protect their privacy in some way, and reinforces the earlier findings that female respondents were more likely than male respondents to have taken steps to improve their online privacy, as well as to both read *and* understood a privacy policy as presented in Tables 5.5 and 5.6, respectively.

Table 5.9: *Access to information on Facebook profiles by gender*

	Friends Only			p-value	Everyone			p-value
	Total	M	F		Total	M	F	
Name Of school	40.70	31.97	48.53	0.006**	24.81	35.25	15.44	< 0.001***
Date of birth	47.29	35.25	58.09	< 0.001***	22.87	32.79	13.97	< 0.001***
Age	44.57	34.43	53.68	0.001**	20.54	31.97	10.29	< 0.001***
Cellphone number	36.82	36.89	36.76	0.981	4.26	7.38	1.47	0.023*
Relationship status	35.66	27.87	42.65	0.012*	14.34	20.49	8.82	0.008**
Blackberry Messaging PIN	40.70	40.98	40.44	0.929	9.30	16.39	2.94	< 0.001***
Home telephone number	17.05	17.21	16.91	0.949	2.71	4.92	0.74	0.048*
Boarding house telephone number	12.02	10.66	13.24	0.524	1.94	3.28	0.74	0.154
Instant messaging contact details	24.81	23.77	25.74	0.716	4.26	7.38	1.47	0.023*
Postal address	15.12	13.11	16.91	0.394	1.94	3.28	0.74	0.154
School email address	22.09	18.85	25.00	0.233	3.49	6.56	0.74	0.015*
Personal / private email address	25.58	22.13	28.68	0.228	6.20	9.02	3.68	0.083
Respondent location	31.40	27.87	34.56	0.247	9.69	12.30	7.35	0.187
Activities and interests	39.92	32.79	46.32	0.026*	14.34	21.31	8.09	0.002**

** significant at the 5% level;** significant at the 1% level;*** significant at the 0.1% level*

In contrast, the 'everyone' column reveals ten out of the fourteen categories in which there are statistical significance in the gender differences. In this instance though it is the male respondents who are shown in every case to be more likely to have the personal data shown in Table 5.8 visible to 'everyone', which means that they are less

likely to have taken some, or any steps to improve their privacy on the *Facebook* platform. This finding, as with the one above, confirms the trend identified of male respondents taking less interest, and/or action in protecting their personal information. This statement is backed up by the findings presented in Tables 5.5 and 5.6, where for example males are shown at statistically significant levels to have been less likely to have taken steps to improve their online privacy, less likely to have read a privacy policy for a social media platform, and less aware of the available *Facebook* privacy settings. The latter is confirmed by the performance of male respondents in this regard as shown in Tables 5.8 and 5.9.

5.4 SUMMARY

In terms of privacy awareness, and privacy in practice (both voluntary and involuntary as discussed) it is apparent that online privacy is an issue that needs addressing. The awareness levels, and significantly the behavioural patterns exhibited by the respondents place large numbers of individuals at high risk levels, in terms of the loss of personal information, vulnerability to exploitation, and even personal harm. The conclusion reached in gender terms is that female respondents generally exhibited more awareness of privacy as a concept, paid more attention to it, and took more action to improve their online privacy. This result is similar to the one obtained in the studies by Marwick et al. (2010) and Steeves (2010), who also determined that female respondents appeared more concerned and proactive about privacy issues than their male counterparts. Male respondents by contrast, displayed what could be interpreted as casual disregard or indifference towards both the concept and mitigation of risk. The behaviour that poses the greatest risk is the relatively high propensity of respondents of both genders, especially males, to engage with strangers. This result is also similar to that obtained by Marwick et al. (2010) who also noted the willingness of youth to interact online with strangers, and that there was "..a need for greater media literacy so that young people can learn how to manipulate privacy settings on social media sites." As discussed throughout this chapter, risk is posed to both individuals and the collective group, so high risk behaviour, even with low overall numbers of participants, is still worthy of the same level of commitment in terms of education and even remedial action.

CHAPTER 6: SEXTING AND CYBERBULLYING

Reference to incidences of sexting and cyberbullying appear with some frequency in the press, usually with reference to specific incidents rather than as a general trend. Despite this the impression is often conveyed that sexting is a regular practice amongst people in the age range of this research group, and that cyberbullying is rampant, especially at secondary schools. Some examples of these incidents are provided in Appendix A. With this in mind, it was decided to assess the levels of these activities amongst the research group. The former activity is directly related to information security (in terms of information disclosure of a personal nature and the consequences thereof), and especially online privacy. Although cyberbullying is less directly related to information security as a whole it is touched upon here, as a relevant consequence of some of the actions described in preceding sections.

6.1 SEXTING

The practice of sexting, as defined in Chapter 2, involves the transmission of sexually explicit material though electronic means. Once an explicit image (or video) for example, has been sent to someone else, the sender no longer has control over it, and this is a major concern in terms of online privacy and information security, for the loss of control / forfeit to another person or persons of compromising material relating to oneself should be considered a serious breach of both the aforementioned concepts. For respondents in the age group considered in this study, the consequences of such breaches at such an early stage of their lives could have long term unwanted effects.

As alluded to above, engaging in sexting has potentially negative consequences for the participants, irrespective of their willingness or otherwise to engage in the practice. Without delving too deeply into these, they include potential embarrassment and ridicule among their peers, outright bullying, emotional distress, sexual abuse, and future compromise through the images or video with employers and universities, as well as other related negative results. An example of the most extreme result of involvement in sexting, and the result of losing control of an intimate image, was the recent suicide of a Canadian teenage girl, fitting the age demographic of the respondents to this study (see Appendix A).

Aside from the negative social and emotional consequences, even for willing participants, under the age of 16, charges of manufacturing, possession and distribution of child pornography could result. The relevant sections of South African law are: the Child Justice Act 2008 (Act 75 of 2008), the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007, the Films and Publications Act 1996 and the Films and Publications Amendment Act 2009. Sanction under these acts has in fact happened under South African law (see item one in Appendix A), and exists alongside other consequences as a potential long term unpleasant side effect of this particular security breach, regardless of the circumstances. While there may be an element of trust, even a strong element of trust at least initially involved in the process of sexting, the above mentioned loss of control and therefore potential breach of trust is ever present, for as Mitnick and Simon (2002:3) stated, people are "…truly security's weakest link."

This research focused on the perceived and actual awareness levels of the term sexting and its meaning, before investigating the related behaviour of the respondents. There were a number of questions relating to this topic in the survey, and the responses were linked as necessary to generate a pattern of behaviour and gather the extent to which the respondents actually engaged in the practice. In line with one of the themes of this research, where appropriate the responses are separated by gender. Results were assessed by frequency of occurrence, and by the determination of p-values for statistical significance. When the number of respondents was very low or an outcome had been established elsewhere, p-values were not calculated.

6.1.1 AWARENESS, PERCEPTION AND INVOLVEMENT

This section addresses the respondents' perception of their own awareness levels relating to the topic of sexting, and assessed their actual awareness of both the terminology, and what the activity involves. Additionally, the respondents' levels of participation, or involvement, in the actual activity of sexting were assessed and conclusions drawn. While respondents were requested to provide answers relating to their involvement in the actions of both sending and receiving, for the purposes of risk assessment in an information security context, the direct action of sending, rather than the more passive action of receiving only was assessed. This was done on the basis that

receiving is less risky behaviour than sending compromising material of oneself, or of someone else, to a third party.

In order to assess the perceived awareness levels of the respondents (before validating them later), Question 76 required respondents to answer 'yes' or 'no' to the question 'Are you familiar with the term sexting?' Of the total number of participants, 72.09% responded that they were familiar with the term, and 15% that they were not, while 13% provided no answer. When this overall figure is broken down by gender, 64.75% of male participants responded in the affirmative, compared to 78.67% of female respondents. By removing the 13% with 'no-answers', the percentage of respondents who indicated their familiarity with the term increased to 82.66%, and the male and female figures increased accordingly, to 78.21% and 86.29%, respectively. A two sample Student's t-test for statistical significance revealed there not to be any statistically significant differences in the answers of male and female respondents (p =0.119), and as such in terms of how the respondents regarded their familiarity with the term sexting appeared not to be influenced by gender. This latter information is included in Table 6.1 as *perceived familiarity from valid answers.* As this was the only question relating to this subject where non-answers were received, all of the other figures are based on the total number of respondents.

Whilst this initial information indicates that the majority of respondents were familiar with the term, this was confirmed, by requiring them to define the term, in the following question, number 77. The definitions provided by the respondents to this question were then compared to the dictionary definition provided in Section 2.2, and a 'correct' or 'incorrect' allocation was given to each response. An answer was scored as 'correct' if the response closely matched the definition, or while not 100% accurate, was close enough to indicate that the respondent did in fact know what they were defining.

An allowance made when examining the responses was that words used by the respondents in place of 'explicit' as per the definition, but which closely matched the meaning of the word were accepted. These included 'gross', 'dirty', 'inappropriate' , 'private' and 'naughty', relating to descriptions of pictures or messages. Conversely, any reference to 'phone sex' without also mentioning either pictures or messaging was judged as 'incorrect', as was any response indicating talking on the phone rather than

messaging. The allowances mentioned above were made to allow for the age of the respondents, and differing attitudes towards sexuality and related terminology. The 'correct' allocations for definitions were then matched with the respondents who has answered 'yes' to Question 76, indicating that they were familiar with the term sexting. These results are displayed in Table 6.1 showing respondent perception versus their actual knowledge in relation to sexting by frequency count.

Table 6.1: *Awareness of and participation in the activity of sexting*

	Total %	Male%	Female%	p-value
Total perceived familiarity with the term (including invalid answers)	72.09 (n=186/258)	64.75 (n=79/122)	78.67 (n=107/136)	#
Perceived familiarity from valid answers	82.66 (n=186/225)	78.21 (n=79/101)	86.29 (n=107/124)	0.119
Acceptable definition	43.02 (n=111/258)	43.44 (n=53/122)	49.26 (n=67/136)	0.351
Admitted participation by terminology	14.34 (n=37/258)	24.59 (n=30/122)	05.14 (n=7/136)	<0.001***
Admitted participation by action (involving themselves)	13.71 (n=34/258)	16.39 (n=20/122)	10.29 (n=14/136)	0.158
Admitted participation by action (involving others)	13.95 (n=36/258)	18.85 (n=23/122)	9.55 (n=13/136)	<0.001***
Admitted participation involving themselves and others	9.68 (n=25/258)	13.93 (n=17/122)	5.83 (n=8/136)	0.032*
Admitted participation by action (incorrect definition and /or unfamiliarity with term)	5.03 (n=13/258)	5.73 (n=7/122)	4.41 (n=6/136)	0.630
Admitted participation in at least one of the sending activities	23.64 (n=61/258)	32.78 (n=40/122)	15.44 (n=21/136)	<0.001***

** significant at the 5% level;*** significant at the 0.1% level*
 # p-value not calculated

The information in Table 6.1 reveals that of those 72.09% of respondents who answered in the affirmative regarding familiarity with the term, only 43.02% were in fact actually aware of what it meant, based on the acceptability of the definition

provided. According to the initial frequency analysis it is evident that female respondents (49.26%) were both more accurate than their male counterparts (43.44%) in their self-assessment, and in their actual knowledge of the meaning of the term. According to p-value however, this difference is not statistically significant.

The data displayed in the *admitted participation by terminology* row, provides the numbers of respondents who admitted to taking part in the activity of sexting when asked as a follow up to Questions 76 and 77, via Question 78: 'Have you ever taken part in sexting?' The *admitted participation by action (involving themselves)* row in the table provides the numbers of respondents who admitted to taking part in sexting in Question 91. This question was intended to elicit an accurate response regarding respondent activity, without the use of the term, to avoid confusion amongst respondents not familiar with it, or who had an inaccurate idea of what the term sexting meant. In this instance the direct question was posed 'Have you ever sent an explicit video or photograph of *yourself* to someone else?

While fewer than half of the male respondents were accurately familiar with the term, 24.59% of them admitted to taking part in the activity when asked to indicate whether or not they had , in contrast to 5.14% of female respondents. A two sample Student's t-test on the results of this question provides an overall p-value of <0.001, and thus the gender differences were genuine and statistically significant at the 0.1 % level. As such it was clear that the male respondents were statistically more likely to have participated in the activity of sexting *in this manner* than their female counterparts, confirming this apparent difference as shown by the frequencies in the table.

For further confirmation of their involvement or non-involvement in the activity, respondents were required to answer in Question 95 whether they had ever sent an explicit video or picture of *someone else that they knew*. This was reflected in the *admitted participation by action (involving someone else)* row of Table 6.1.

The data in the second last row of Table 6.1, *admitted participation by action (incorrect definition and /or unfamiliarity with term)* denotes the respondents who had responded positively to sending an explicit picture or video of themselves (Question 91), but who had answered 'no' to being familiar with the term sexting in Question 76, and whose definition of the term had been incorrect in Question 77. The purpose of this row is

again to test actual behaviour against perceived knowledge, and to make allowances for unfamiliarity with the terminology preventing an accurate answer in behavioural terms. Whilst there is a difference in the frequencies recorded for this behaviour, with male respondents (5.73%) exhibiting higher levels of participation than female respondents (4.41%), the gender difference in this case was is statistically significant, as shown by the p-value of 0.630.

The differences in both male and female respondents' overall responses in the *perceived awareness* and *acceptable definition* rows reveal that the respondents' perception of their own knowledge or awareness (through their professed familiarity with the term sexting) is not matched by their actual demonstrated knowledge in terms of understanding of the term sexting, and therefore possibly the implications of engaging in the activity. It could therefore be stated that the respondents across both genders were less aware in actual terms than in their perception of their own awareness; a result which is consistent with the results obtained from the analysis of the awareness of threats in Chapter 4.

When asked to identify their own behaviour in the absence of the terminology, the results show a degree of consistency across the three relevant rows, with numerical differences (in combined gender numbers) of 37 (14.34%) admitting *participation by definition*, 36 (13.95%) admitting participation involving *someone else whom they knew* and 34 (13.71%) admitting participation involving themselves. A statistically significant gender difference is apparent here, with a Student's t-test indicating that male respondents were more likely to take part in sending material of other people than their female counterparts. The consistency described above suggests the possibility that those learners who engaged in the practise, not only shared explicit material of themselves, but of others as well. However, whilst this remained a possibility, the figures in the row *admitted participation involving themselves and others* indicated that *fewer* respondents had been involved in sexting pictures of themselves *and* other people that they knew, than the individual tallies for those activities (with a statistically significant gender bias towards male respondents at the 5% level). An interpretation of this is that when performed, sexting is either done via sending an explicit picture of oneself, or by sharing pictures of someone else with a third party. Bothe examples have dangerous connotations, although the latter is a potentially dangerous result in itself, in

that pictures of learners were in fact being passed on to third parties. The consent or otherwise of this activity is discussed in Section 6.1.2.

To gain a more accurate number of the actual participants, a count was done of all respondents who had indicated that they had taken part in any activity relating to sexting, across Questions 78, 91, and 95. A respondent who answered yes to any one of those questions was allocated a positive score, resulting in a total participation number of 61 respondents, or 23.64%, which is 9.93% higher than the number who had admitted participation by sending material of themselves, and 9.69% higher than those who admitted participation by sending material of someone else that they knew. This is reflected in the row titled *admitted participation in at least one of the sending activities* in Table 6.1.

Broken down by gender, 32.78% of male respondents had taken part in sexting via one or more of the means included in the questions relating to participation, as opposed to 15.44% of female respondents. This follows the trend throughout Table 6.1, of males having higher admitted participation rates than females, but with female respondents having higher percentages in familiarity with the term, and correctness of their definition. A Student's t-test on the overall participation figures as provided above, indicate that the difference between male and female respondents was indeed statistically significant, with a p-value of <0.001 which is significant at the 1% level, and thus male respondents were more likely to have participated in any of the forms of sexting activities than females.

There are two conclusions that could be drawn regarding participation in and awareness of sexting. The first of these is that overall, perceived awareness was higher than actual awareness across both genders. The overall percentage of only 43.02% of all respondents being able to correctly define the term indicates a concerning gap in their awareness, and this is an area that would require particular attention in any relevant education or awareness initiative. With fewer than half of the total respondents having actual knowledge of the meaning of the term, the potential for vulnerability is greatly increased, although the comparatively low overall participation figure of 23.64% and the 5.03% participation level of those who neither knew the term nor had the correct definition does indicate that a lack of awareness does not correlate directly with

participation. Of interest however, is the fact that 12.40% of all respondents indicated via Question 97 that they had received an explicit photograph or video from a friend, which was only marginally below the 14.73% of combined responses to having received an explicit video or photograph from a boyfriend (5.04%) or girlfriend (9.69%). This provides further evidence that sharing of material between learners was taking place.

In terms of risk, it could be stated that with a total participation of 23.62% and thus almost one out of every four respondents having participated in some way, the potential for the unwanted consequences described previously is significant enough to warrant concern, as is the possibility that the numbers of participants could potentially increase, based on existing figures.

In terms of comparison, Rice et al. (2012) performed a study on school learners of a similar grade range used in this survey. They produced the result that 15% of their respondents had taken part in sexting, although they did not differentiate between self-participation and participation involving others. Another survey, conducted in 2008 by the (US*) National Campaign to Prevent Teen and Unplanned Pregnancy* (The National Campaign 2008) on 13-19 year olds (which is a broader age range than the respondents in this study) , revealed that 39% of their respondents had taken part in the sending of *sexts*. This figure was further broken down by gender, with 37% of female respondents, and 40% of males having participated in s*exting*. These figures dropped though when filtered to show only those who had sent explicit material of themselves: in this case 20% of the respondents had done so, of which 22% were female respondents, and 18% males. Both sets of results indicate a similar gap between genders of 3% and 2%, respectively, which is a much smaller gap than amongst the respondents to this questionnaire.

Comparison between the sexting trends identified in this research, and that of the *National Campaign to Prevent Teen and Unplanned Pregnancy,* shows similarity in the overall participation levels, while the gender difference is (in terms of percentages) smaller. There is however no evidence provided relating to the statistical significance or otherwise of this gender result. The study conducted by Rice et al. (2012) revealed a lower overall participation rate, but failed to differentiate between genders. In terms of context, both the *National Campaign to Prevent Teen and Unplanned Pregnancy* survey

and the one conducted by Rice et al. (2012) took place in the United States of America, with significantly larger sample sizes, and with age ranges (between the two surveys) ranging from 10 years old to 18, all of which would have impacted on the results obtained.

While it could be argued that knowledge of the behaviour is more important than knowing what the correct definition of the term is, the two are often linked, and should be so in any information security awareness or education campaign that may seek to redress this knowledge gap (in terms of terminology and behavioural awareness) in such a potentially damaging aspect of information security behaviour. In terms of mitigating this risk, the evidence presented confirms that the emphasis should first be on the action and consequences of sexting itself, following on from the initial explanation of the meaning of the term.

The second conclusion drawn from the evidence presented is that, in terms of participation, male respondents had a higher participation rate than female respondents, as evidenced by the frequencies on display in Table 6.1. This is evidenced by both the overall participation p-value as noted previously and p-values revealing statistically significant gender superiority of male respondents for participation involving others, admission of participation by the use of the term (both significant at the 0,1% level), and in cases of sexting involving themselves and others. It can be inferred from these results that male respondents were perhaps more likely to share images received with other males, than their female counterparts, which could account for the significant gender difference in terms of participation involving others.

Overall then, it can be stated that sexting is more prevalent amongst males, and that the practice itself, is not as common amongst learners of the target group as might have been assumed based on popular opinion, and reports in the press. There remains however, a serious need for education in order to mitigate the potential harmful consequences of participation, including potential legal sanction.

6.1.2 SEXTING BEHAVIOUR

Having established the extent of the respondents' participation in the practice of sexting, this section investigates further the nature of the behaviour of those who had

participated. While it has been established that the activity is itself, in any form, a threat to the participant's personal information security and online privacy, aspects of the behaviour that enhance the risk are examined. As in the previous section,, the focus is primarily on sending rather than receiving behaviour.

In Question 92, ('Did you do this …'), respondents were asked as a follow up to the preceding question on their involvement, to supply answers relating to their behaviour when sexting, the results of which are given in Table 6.2.

Table 6.2: *Frequencies of specific sexting behaviour*

Request Behaviour	Count*(n=258)*	Frequency %
By request	26	10.08
Without being requested	10	3.88
More than once?	15	5.81
Because you felt pressurised to do so	4	1.55
To an older person	8	3.10
To a younger person	7	2.71
Not Applicable	217	84.11
Other (option available for open-ended answer)	10	3.88

In terms of risk the numbers are low, but as previously established the activity itself is a risk to personal information security and online privacy and the answers received serve to illuminate this. While participating by request would seem perhaps one of the more innocuous methods of doing so, the risk in losing control over the material sent has been established. A greater risk is that there are respondents who indicated that they sent explicit material without being requested to do so. This shows an increased risk of compromise or misuse of the material due to no negotiation regarding the receiver's use, storage or distribution of the material, as would perhaps more likely be the case if

the material was requested. The fact that some respondents (5.81%) engaged in the activity more than once showed that they were either unaware of the risks, or chose to ignore them.

The number of respondents who answered that they had felt pressured to send an explicit picture or video was low; 4, or 1.55% of all respondents. While it could be considered positive that the majority of those participating in the activity were doing so apparently free of duress, respondents who did participate under any degree of duress would potentially have an even lesser chance of maintaining their privacy, owing to the potential absence of a trust relationship with the receiver.

While not necessarily under duress, a concerning (in terms of risk) result was obtained by analysing the responses to Question 96 (which dealt with the distribution of explicit material of someone else), in conjunction with the results shown in Table 6.1 for this behaviour. This indicates that 8.91% of respondents had distributed material of someone else without that person's consent, compared to 3.49% who had received consent to distribute. While the values are relatively low in overall terms, high numbers are not necessary for participants, even unwitting ones to be at risk of compromise via non-sanctioned distribution. Even the granting of consent for someone else to distribute compromising material to a third party or parties is high risk behaviour, and one that would need to be investigated in more depth in future research.

Table 6.3 reveals who the receivers of explicit images or videos were for those respondents who had indicated that they had sent such material of themselves. The information in Table 6.3 was compiled from the answers to Question 93, which tasked the respondents with providing an answer to 'Who did you send it to?' The majority of respondents (12.79%) had sent material to either a boyfriend or girlfriend, which implied a degree of trust, which as previously emphasised could be temporary. This is because once such a relationship has ended, the trust aspect could be broken, and the sender would be at a potentially high risk of having their material distributed to third parties, or used in other compromising ways. The percentage of those sending material within what could be termed a situation or relationship of trust was increased to 18.21% when adding those who had sent to a friend. While this is relatively positive considering that 84.11% of respondents had provided 'non-applicable' as the answer, it

could be argued that as noted previously, trust relationships can break down and potentially pose an equal if not greater risk in terms of vindictive or non-sanctioned re-distribution of the material.

Table 6.3: *Targets of specific* sexting *behaviour*

Recipient	Count (n=258)	Frequency %
Your boyfriend	15	5.81%
Your girlfriend	18	6.98%
A friend	14	5.43%
An acquaintance	5	1.94%
Someone met online and not in person	6	2.33%
Not Applicable	217	84.11%
Other (option available for open-ended answer)	5	1.94%

The greatest risk in terms of behaviour drawn from Table 6.3 is that six respondents had sent explicit material to someone that they had never actually met. Sending to significant others has some risk associated with it, for example what happens to the material following the break-up of a romantic relationship or friendship. The risk is greatly increased however when the sender has no knowledge of the receiver other than via online means (either through information obtained from the stranger themselves through communication, or information available online, neither of which would necessarily be truthful). While not numerically or statistically significant, the fact that there were six respondents who admitted to doing this was in itself reinforcement of the need for education regarding the risks of participation in this activity as outlined previously.

Possibly the primary threat to respondents in terms of sexting outside of a romantic relationship is the social engineer (whether witting or unwitting, since fellow learners may play the role of social engineer in terms of the behaviour outlined below without being aware of the formal name for it). Previously defined in Chapter 2, in terms of direct relevance to sexting, it is worth emphasising here the manipulative nature of the social engineering. Particularly pertinent is the fact that the actions of the social engineer are seldom in the other person's best interest.

The latter point holds immediate relevance to information security in general, and certainly directly to sexting, where a person known or unknown (whether fellow learner or someone external) to the learner could persuade them to take an action , in the form of sending compromising material of themselves, which would certainly not be in their best interest. Those learners who sent explicit material to people whom they had not met other than online, could well have been the victims of social engineering, deliberate or otherwise. Learners could also be vulnerable to an aspect of social engineering called pretexting. Taking this attack vector into consideration, a strong emphasis should be placed on the idea that not everyone online is who or what they appear to be, and learners should therefore be warned against, for example an alleged peer (age and/or interest wise) with whom they become familiar online, for that person may in fact be neither the age nor the gender that they claim to be.

In terms of the risk of social engineering, 13.56% or only 35 respondents out of the 258 claimed familiarity with the term as shown in Table 4.2. While the survey provided no measure of their actual knowledge or understanding of the term, it could be said that in terms of perceived awareness alone the risk level amongst this group of respondents to various forms of social engineering attacks is relatively high conceptually. However, the relatively low figures of (sexting) engagement with people not known to them physically could indicate a greater awareness of the dangers of dealing with, in sexting terms only, such strangers. If so, this could be considered positive behaviour, when viewed in the context of the findings shown in Chapter 5, which revealed high levels of interactions with strangers.

6.1.3 SUMMARY

The number of sexting participants was low, and the majority of participants sent images to people known to them, with whom it could be said there was some kind of trust relationship, whether implied, tacit, or vocalised. While the practise did not appear to be endemic in this respondent group, the risk to the individual(s) involved is not reduced by low numbers, owing to the potential impacts of participation and the recommendation regarding the importance of mitigating this risk through education remains. The importance of addressing the consequences of indulging in this practice cannot and should not be underestimated.

6.2 CYBERBULLYING

The inclusion of cyberbullying as a separate section was done in order to present it as a consequence to the actions of the respondents in the previous chapters and sections, specifically those relating to online privacy, and sexting. While the material is available from the results of the questionnaire for deeper analysis, this was considered out of scope other than in the context of consequences of action. The goals of this section are to establish the extent of cyberbullying amongst the respondents, and to identify from where the risk is highest in terms of perpetrators and victims.

Question 79 required the respondents to indicate whether they were familiar with the term cyberbullying. This term was defined in Chapter 2, but a further definition provided by Wilson (2006) describes cyberbullying as the "…sending or posting harmful or cruel text or images using the Internet or other digital communication devices." (The term refers to bullying through these mechanisms in a social, emotional and psychological rather than physical sense, although the latter can be a consequence of cyberbullying. Unlike the use of the term 'encountered' used in Chapter 4, the term 'familiar' implied more than simply having heard of the term; they there should be a degree of understanding of the concept inherent in the 'yes' answers. The responses received indicate that 231 respondents, or 89.53%, claimed familiarity with the term. The respondents were then asked to provide a description of the meaning of the term.

Of the descriptions provided by the respondents which were compared with the definition, those that fitted the definition in a broad sense, and included words such as 'online', 'social media', 'electronic communications' in conjunction with 'bullying' were accepted. Those that either mentioned bullying with no additional context, or made no mention of a connection with a use of technology were rejected, as were other inappropriate answers. The results of this comparison are indicated in Table 6.4, showing that the overall understanding of the term cyberbullying stood at 79.06%, a number almost 10% lower than the 89.53% of respondents who pronounced themselves familiar with the term. Understanding of the term was high amongst respondents of both genders. These figures showing high levels of understanding of the term cyberbullying stand in contrast to results obtained by Li(2006), whose results showed that in that study, 55.6% of male respondents and 54.5% of female respondents understood the term. Potential reasons for this difference include the lower age of the respondents in Li's study, and that learners have become more aware of the issue over the six year gap between that study and this one.

Worth noting as this point is that of the total respondents, 79.19% indicated in their answers to Question 19, that they primarily used their cellular telephones to access their social media platforms. This would have provided them with more frequent access than would have been the case if they had used mainly computers, as depending on the rules (if any) regarding cellphone access at the schools, the respondents would potentially have had unlimited access. The downside of this more frequent access was that the potential for constant or sustained abuse or harassment is increased, with respondents potentially able to receive images, and messages throughout the day and night.

Question 81 required respondents to select which of three options was the most appropriate regarding their experience of cyberbullying. The options provided, in answer to the question 'Have you ever experienced cyberbullying were: 'Yes I have been on the receiving end', 'Yes I have been involved in doing the bullying', and 'I have been on both the bullying and receiving ends'. Whilst the respondents were instructed to select at least one option, it was confirmed that of those who indicated that they had been on the receiving end of cyberbullying, only three had also selected the option that

they were involved in both. Similarly of those who indicated that they had done the bullying, only two had also selected the option for both.

It can be concluded therefore that the figure of 36 respondents involved in both bullying and being bullied actually added to the separate numbers displayed for each of those activities, while not providing a fully accurate alteration to each figure. Despite this it is clear that the numbers involved in perpetrating, and in being victimised were higher than indicated in Table 6.4.

Table 6.4: *Awareness and involvement levels in cyberbullying by terminology*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Perceived Understanding of cyberbullying	231	89.53	107	87.70	124	91.17	0.368
Accepted Definition	204	79.06	95	77.86	109	80.14	0.547
Respondents admitting being bullied	40	15.50	24	19.67	16	11.76	0.083
Respondents admitting to being bullies	7	2.71	6	4.91	1	0.42	0.048*
Respondents bullied, and involved in bullying	36	13.95	23	18.85	13	9.55	0.034*

** significant at the 5% level*

What is indicated though, is that while incidences of cyberbullying as per the definition understood by the respondents were not endemic to the group of respondents, there were certainly instances of it, and that makes it an issue worth addressing. One respondent bullied should be considered one too many, for the results can be tragic (see Appendix A). Thus with a number of approximately one in six respondents having been victims of cyberbullying the problem should certainly be considered serious enough to warrant education and intervention.

Notably in terms of gender differences, the significant results are that male respondents were more likely to admit to being a bully (although the numbers involved were so small as not to constitute an accurate sample), and were more likely to have been involved in bullying and being bullied. This result is consistent with the finding s of

Li (2006). There is no significance in the difference between the genders in terms of who experienced bullying to a greater or lesser extent.

Taking into consideration that the definition includes the word 'repeated', the information revealed via Question 85 should be both noted, and as far as possible placed within context : The question asked respondents if they had ever received an abusive or unpleasant message. The response to this was that 111 (43.02%) had received such as message, which is a figure significantly higher than those who had admitted being victims of cyberbullying. That said however,, it was not determined whether an occurrence was a once-off or repeated occurrence (which would mark it as bullying rather than simple unpleasantness, as per the accepted definition). As such while not possible to conclude that more cyberbullying was taking place than initially apparent, it is also not worth discarding the volume of those who had received such a message.

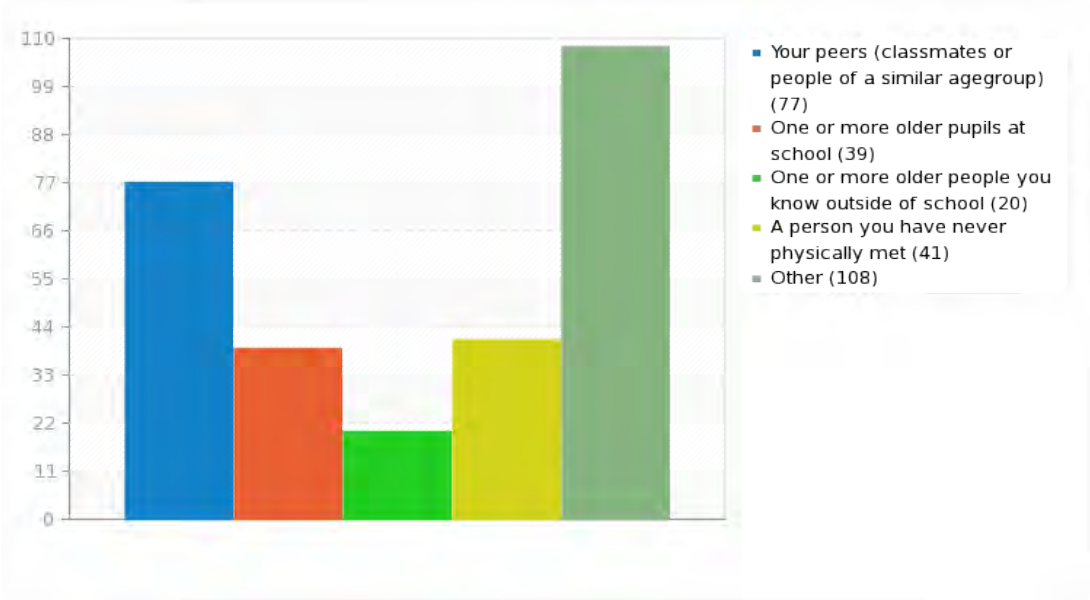

***Figure 6.1**: Perpetrators of cyberbullying or the sending of abusive/unpleasant messages*

Figure 6.1, illustrating the answers to Question 87, shows the categories of people from whom respondents had experienced cyberbullying and/or received abuse or unpleasant messages. In answering this question, the respondents were able to select more than one option, for it could have been the case that they had been cyberbullied or received abusive messages from more than one category of perpetrator. As a result, the numbers

denoted in Figure 6.1 represent a combination of responses rather than absolute numbers. What is clearly indicated here was that if the 'other' category was excluded (due to almost all respondents providing 'not applicable' when asked to specify, if they had selected 'other' as their answer), the majority of perpetrators (29.84%) came from within their peer group. This result is unsurprising considering the age of the respondents, and the nature of social interaction within that age group. More alarming however, is the 17.05% of respondents who indicated that the perpetrator was someone they had never physically met, which places them in the earlier defined category of 'stranger'.

In terms of strangers, Table 6.5 shows the numbers of respondents who reported being bullied by strangers (as per previous definition of the word), and how it corresponded with their previously established behaviour patterns regarding strangers. The information was taken from Tables 5.1 and 5.2, as well as Question 87.

Table 6.5: *Relationships between interaction with strangers and cyberbullying*

	Total(n=258)	%
Engaged in communication with stranger	117	45.34 (n=258)
Engaged with and bullied by stranger	27	23.07 (n=117)
Friend request from stranger accepted	159	61.62 (n=258)
Stranger's Request accepted and bullied by stranger	17	10.69 (n=159)

The first row repeats the overall number and percentage of respondents who had admitted to engaging in communication with a stranger, while the next row shows the overall number of participants who had both done that *and* indicated that they had experienced cyberbullying or online unpleasantness from a stranger. The 23.07 % is calculated from the count in row 1, and those who had engaged in communication, rather than from an overall percentage of all respondents. This shows that almost one in five respondents who had engaged in communication with a stranger had experienced

cyberbullying and/or online unpleasantness from a stranger. This serves to emphasise the pre-established risk of such interaction.

Less risky perhaps in numerical terms is the 10.69% of respondents who had accepted the 'friend' request of a stranger, and also experienced cyberbullying or online unpleasantness. Continuing with the assertion that no number is too insignificant to pose a risk, considering the wellbeing of the individual, this figure also serves to emphasise a link, albeit not such a firm one between the behaviour displayed and the consequences thereof. Despite this, and the emphasis placed in this section and elsewhere on stranger interaction, the numbers in Figure 6.1 indicate that the greatest threat in terms of cyberbullying and related actions came from within the peer group, and within the school environment, an outcome which would, as stated require education, as well as intervention and remedial action where possible.

Table 6.6: *Perpetrators of cyberbullying / unpleasant online behaviour by gender*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Bullying / unpleasant online contact from peers	77	29.84	39	31.97	38	27.94	0.575
Bullying / unpleasant online contact from older people within the school environment	39	15.12	17	13.93	22	16.18	0.616
Total Perpetrators within Peer group / school Environment	116	44.96	56	45.90	60	44.11	0.774
Perpetrator was a stranger	41	15.89	20	16.39	21	15.44	0.835
Perpetrator(s) were the same gender as the victim	90	34.88	46	37.70	44	32.35	0.370

Having established the primary sources of risk, a brief examination of whether one gender was more at risk from cyberbullying and/or online unpleasantness was carried out. The gender of the perpetrators was also examined. These results are provided in Table 6.6.

As is evident from Table 6.6, the numbers and percentages of male and female respondents who received unpleasant contact from peers, and those who received it

from older people within the school environment are very similar. This is confirmed in the third row of the table, where the two categories above it were combined to form an overall picture of the school environment. Similarly row 4, which shows the gender breakdown of respondents who had suffered some form of online victimisation from a stranger, also give an almost identical breakdown figures by gender. These results indicated that neither male nor female respondents appeared more likely than the other to experience cyberbullying or online abuse or unpleasantness. The p-values determined confirm this finding, indicating no statistical significance of these results. Noticeably too, there is no indication that either gender was more or less likely to experience such behaviour from their own, or the opposite gender.

6.2.1 SUMMARY

Summarizing the preceding discussion, it is clear that cyberbullying and related behaviour was just as prevalent amongst male and female respondents the perpetrators were primarily within the school environment (and peer group), and that gender played no significant role in determining either victimhood, although male respondents were more likely to be guilty of perpetration. Considering this, education should be directed toward both information for victims regarding appropriate actions, and education regarding the negative results of perpetration.

CHAPTER 7: PASSWORD HABITS

Questions 64 to 75 dealt with the respondents' attitudes toward password security and their password usage in practice. The computer logon password could be considered as one of the more important pieces of information to keep secure, since if it were to be compromised, access to a user's entire system could be compromised. While poor password security may not be the highest risk facing the respondents, it nevertheless poses a significant risk.

In the majority of situations faced by the respondents, the password could be considered the first line of defence against compromise of information and /or breaches of privacy, as this is the gateway not only to the respondents' computers, and computer based files, but also to their social media accounts and potentially their financial accounts too. The compromise of any of these could result in information theft and distribution, social compromise, loss of data, financial distress and invasion of privacy.

7.1 PASSWORD CONSTRUCTION

This section deals with the physical makeup of the respondents' password(s) and compares them with established best password practice. Also covered is how the respondents treat their password(s) in terms of protection, and therefore the security, integrity, and privacy of their information in whatever form. Gender differences were tested for statistical significance as appropriate. With the exception of the first question which specified 'computer logon password', it is worth noting that the term 'password' was used on all questions without specifying which password. As such some degree of latitude was afforded to the respondents in their answers, in terms of whether they based their answers on a single specific password, or on their general password practice.

7.1.1 PASSWORD LENGTH

Current wisdom states that the longer a password is, the more secure it is. This is certainly so in the case of a *brute force* password attack, where, as noted by Dell'Amico, Natipoles, Michiardi and Roudier (2010), the attack begins with a blank password and then varying combinations of increasing length are tried until success is achieved. The

respondents were asked to select the length of their password from a pre-determined list in Question 64.

Table 7.1: *Different password lengths*

Password length	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%
5 Characters or less	36	13.95	22	18.03	14	10.29
5-10 Characters	165	60.46	72	59.01	93	68.38
Longer than 10 characters	56	22.09	28	22.95	28	20.58

As is evident from Table 7.1, the majority of the respondents' passwords fell into the 5-10 characters length category, which is in agreement with the average password length noted by Dell'Amico et al. (2010) of 8 characters. Noticeably the majority of selections by both male and female respondents are consistent with the overall percentage. The Open Web Application Security Project (OWASP 2012) recommends that in terms of risk, the minimum length of a password should be 8 characters, and also notes the potential for this in delaying a *brute force* attack. This recommendation was supported by Microsoft (2009). With 22% of all respondents having submitted that they employed passwords longer than 10 characters, a degree of awareness and responsibility was revealed, although not an encouraging one overall. A comparison between those who used these longer passwords, and those who indicated familiarity with the term 'passphrase' (Question 69) is included in the results in Table 7.4. If the rows 1-3 in Table 7.1 were classified by level of risk, as high, medium, and low respectively, the majority of respondents based on password length *only,* would fall into the medium risk category.

7.1.2 PASSWORD CHANGE FREQUENCY

The next assessment of password security revolved around how often the respondents changed their password(s). Table 7.2 indicates that the majority of respondents revealed poor password practice by indicating that they never changed their password(s).

***Table 7.2**: Frequency of password changes by respondents*

Frequency	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Monthly or more often	69	26.74	32	26.22	37	27.20	0.860
Once or twice a year	58	22.48	23	18.85	35	25.73	0.184
Yearly	30	11.63	19	15.57	11	8.085	0.656
Never	101	39.15	48	39.34	53	38.97	0.951

Changing passwords with some degree of frequency provides improved security as stated by Granger (2002), and the more sensitive the data being protected by the password, the greater care should be taken to protect the password. As such, the majority of respondents were at risk of password compromise simply by not changing their password(s). As indicated by the p-values given in Table 7.2, there are no statistically significant differences between male and female respondents in terms of frequency of changing their passwords. As per Table 7.1, if the categories of answer were changed to risk assessment categories of low for *monthly or more*, average for *once or twice a year*, high risk for *yearly*, and extreme risk for *never*, the majority of respondents would be at the extreme risk level of potential compromise owing to poor change frequency.

7.1.3 PASSWORD REUSE

Question 67 required respondents to select an option in response to 'Do you use the same password for:' These options were 'I have separate passwords for each account', which appears in the table as *separate passwords for each account*; 'more than one account (i.e. computer logon and instant messaging logon)', which appears in the table as *same passwords for more than one account,* and 'all of your accounts', which appears in the table as *same password for all of their accounts*.

***Table7.2**: Number of passwords according to account usage*

Frequency	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%
Separate passwords for each account	81	31.40	39	31.96	42	30.88
Same passwords for more than one account	150	58.14	66	54.09	84	61.76
Same password for all of their accounts	27	10.47	17	13.93	10	7.35

The primary feature of Table 7.3 is that the majority of respondents selected the option indicating that they used the same password for more than one account. If only the 10.47% who answered so, used the same password for *all* of their accounts, then the 58.14% of respondents using the same password for more than one, *but not all* of their accounts indicates positive awareness and resultant good practice regarding password security.

That there were respondents who indicated the use of only one password for all of their accounts however, provides some evidence of lack of awareness and/or disregard for the notion of password security. It should be noted that owing to difficulties (real or perceived) in remembering passwords, especially multiple ones, factors such as these could have played a part in the multiple use of a single password, as opposed to direct lack of awareness or disregard for security.

Encouragingly, almost a third of all respondents used separate passwords for each of their accounts. This action confirms that there was indeed a higher degree of awareness and the need for password security amongst the respondents as a group, and that, for this 31.4% the awareness had translated into action. Following the same pattern as Tables 7.1 and 7.2, in terms of password security, the information in this table could be regarded in terms of risk as: low (respondent used separate passwords for each account), medium (respondent used the same passwords for more than one account); and high (respondent used the same password on all their accounts). Then the majority of respondents, across both genders, would fall into the 'medium' category.

7.1.4 PASSWORD CONSTRUCTION BY CONTENT

Investigating the respondents' knowledge of password security more deeply, they were tasked in Questions 70 and 71 to provide more detail about their password construction. Question 69 queried their familiarity with the term 'passphrase'. The initial question dealing with familiarity or otherwise of the term 'passphrase', yielded the result that only 23.64% of all respondents indicated familiarity with the term. Passphrases are defined by Keith, Shao, and Steinbart (2009) as "...long passwords created from multiple words to form a phrase." The benefits of this include the increased security of password with many characters, but which is relatively easy to remember, especially in comparison to other long multi-character passwords.

***Table7.3**: Respondents' construction of passwords*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%
Passphrase familiarity	61	23.64	39	31.96	22	16.17
Longer than 10 Characters	56	22.09	28	22.95	28	20.58
Dictionary word	48	18.6	18	14.75	30	22.05
Combination of two or more words	76	29.46	31	25.40	45	33.08
Sentence (not separated by spaces)	15	5.81	8	6.55	7	5.14
Combination of words, numbers or letters and other characters	129	50.00	62	50.81	67	49.26
Numbers only	29	11.24	15	12.29	14	10.29
Respondent's date of birth	25	9.69	12	9.83	13	9.55
A significant other's (boyfriend or girlfriend) date of birth	8	3.10	3	2.45	5	3.67
A family member's date of birth	15	5.81	7	5.73	8	5.88
Respondents' Name	50	19.38	28	22.95	22	16.17
A significant other's (boyfriend or girlfriend) name	22	8.53	7	5.73	15	11.02
Someone else's name	44	17.05	11	9.01	33	24.26
A pet's name	40	15.5	13	10.65	27	19.85
A telephone number	14	5.43	6	4.91	8	5.88
The word 'password' , the numbers '1234' or a blank password	16	6.2	6	4.91	10	7.35
None of the above	131	50.78	71	58.19	60	44.11

Unlike when dealing with the term sexting, respondents were not asked to provide a definition, as a follow-up. Additionally there was no direct action with which to confirm respondents' knowledge or otherwise of the term 'passphrase' alongside a definition, other than by comparing the users of longer passwords from Question 64 with those who indicated familiarity with the term 'passphrase'.

For this purpose the row from Table 7.1 indicating respondent's with passwords 10 characters or more in length has been repeated on Table 7.4 directly beneath the row showing figures for familiarity or otherwise with the term 'passphrase'. Numerical and percentage based comparison reveals that superficially at least there is a certain amount of consistency between those using the longer passwords and those who professed familiarity with the term. However, once analysis was carried out to determine how many respondents had professed familiarity with the term *and had* made use of passwords made up of ten or more characters the results implies that the apparent consistency between the use of passphrases and the use of longer passwords as shown in Table 7.5 to be almost co-incidental.

Table 7.5: *Difference between familiarity y with and use of passphrases*

	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%
Use of longer password s and familiarity with the term 'passphrase'	15	5.81	10	8.19	5	3.67

What is revealed then is that there is almost no correlation between knowledge of the term 'passphrase' *and* the employment of an actual passphrase. In terms of awareness, this indicates a serious gap between knowledge and practice, which could have been the result of actual lack of knowledge of the term, as opposed to the perceived knowledge indicated by the respondents.

It is therefore acknowledged that there is the possibility that, as was the case with sexting, *fewer respondents* than those who indicated familiarity were in fact correctly familiar with the term. Those using ten character or longer passwords may have been doing so *in spite of* their lack of knowledge of the term, rather than owing to familiarity with it. Nonetheless, the results produced indicate that the majority of respondents,

across both genders were unfamiliar with the term, and therefore less likely to be making use of passphrases as a means of enhancing their password security. This is so despite the 22.09% of respondents who indicated their use of the longer (10 or more characters) password(s), bearing in mind that longer passwords and passphrases are not synonymous. While this alone does not automatically weaken the quality of the respondents' passwords, it is a figure worth noting in terms of awareness or lack thereof, both in overall terms of information security, and passwords specifically. The understanding of the term (and the employment of good password practice) was further assessed by the next two questions on password construction.

The password vulnerability of respondents in terms of how they constructed their password was assessed, initially via Question 77, which required the respondents to select how their passwords were constructed, given a list of options. These are shown in Table 7.4. Encouragingly, exactly half (129) of all the respondents answered that their passwords consisted of *a combination of words, numbers or letters and other characters*, which was the strongest or most secure option available for that question. The gender split in this instance was almost even, with 50.81% of male respondents selecting this option, and 49.26% of female respondents selecting this option. This result is positive from an actual security practice point of view, showing that respondents have taken action to make their password(s) more secure. By inference then, this must have been done as a response to having a level of awareness about the importance of password security. While this is an encouraging result, as stated, it is still an area of concern, due to half of the respondents not using the most secure forms of passwords.

Contrary to this positive result, 18.6% (nearly one out of every five) of all respondents used what could be considered the weakest password: a simple dictionary word, leaving them very vulnerable to *brute force* or *dictionary attacks.* Notably few respondents: 4 (1.55%) used both a dictionary word *and* had a password length of five characters or less, which is one of the two weakest combinations possible from the options provided. The other weakest combination was the use of only numbers (11.24%) *and* a password length of five characters or less. For this combination there were again a small number of respondents: five(1.93%). In contrast, 35 respondents (13.56%) made use of the strongest combination, being a combination of words, numbers or letters and other characters *and* a password consisting of ten or more characters.

Despite the fact that there were higher number of respondents with the most secure option, than with the least secure option, the problem remains that the figures themselves are very low, showing poor password practice and/or *threat awareness* levels amongst the respondents. The fact that for example nearly one out of every five respondents made use of a dictionary word is an indicator of the need for education around the importance of what should be the most basic of security concepts: the password. That said, the number of respondents who selected either *a combination of two or more words* or *a sentence (not separated by spaces)* shows that while risk was present the majority of respondents were not operating at the most vulnerable level in terms of password security.

If the latter two password construction options from the preceding paragraph are combined to form a single risk category called 'medium', the combination of words, numbers or letters and other characters would form a risk category called 'low', and the dictionary word and number categories were joined to form one called 'high', then overall, the risk level for the majority of the respondents would be ranked as 'low' owing to the 50% who fall into that category. Despite this, and the 35.27% falling into the aforementioned 'medium risk' category, the overall result is that there is still sufficient risk to warrant a focus on awareness education in terms of length and password construction.

Aside from the risks in password construction, there are other choice based risks associated with passwords. Two of the greatest of these are linked, namely and are guessing, based on knowledge about (or obtained about) the person, and through the obtaining of the actual password. Both of these are risks due to aspects of social engineering, as explained in Chapters 5 and 6.

Techniques relevant to password security for the respondents, and which are used in social engineering attacks include *shoulder surfing* (Long 2008) where an attacker simply observes what a target is doing from behind (such as watching someone typing in a password, or visually obtaining the information through the sighting of a note near the computer screen on which a password has been written, for example), and elicitation. Though the term 'attacker' is used, it should be noted that this could be anyone, and in the context of the schools could be, as with sexting, a fellow learner or

teacher, someone external, or just as possibly someone known to the learner as someone unknown.

Examining risk from poor password practice from a different perspective, when the respondents were required to select from provided options, as to whether their passwords conformed to any of a set of low security, common password options, the result (see Table 7.4) is more positive in security terms. The options provided were: *the respondents' own date of birth, a significant other's (boyfriend or girlfriend) date of birth, a family member's date of birth, the respondents' own name, a significant other's (boyfriend or girlfriend) name, someone else's name, a pet's name, a telephone number, the word 'password' , the numbers '1234', a blank password, or none of the above.*

A total of 50.78% of all the respondents selected the 'none of the above' option, which is a positive figure in terms of password selection. Less positive though is that just less than 20% of respondents used their own name as a password. For friends, acquaintances, strangers and social engineers both known and unknown, this would be the simplest guess, from the list of simple guesses provided to the respondents. Overall, the results show that almost half of the respondents were using these common options for passwords.

If the consequences of password compromise are not well known, then the risk of falling victim to something as simple as a request for a password, whether through social engineering, or more explicitly electronic means such as through targeted phishing, spam emails and text messages, or requests from within the peer group, is greatly increased. With regard to guessing, the more information that the person doing the guessing has about the person whose password they are trying to guess, the easier the guessing process becomes.

7.1.5 SUMMARY

In terms of password construction and vulnerability, with half of the respondents using common options for passwords, just under one fifth using a dictionary word, and with the majority of respondents using the same password for more than one account, and/or admitting to never changing it, the risk level could be regarded as high. This is primarily because even though in some cases there is evidence of good password

practice, this is never higher 50% of the respondents. As noted throughout this section, education in this area would be highly recommended for this group of respondents.

7.2 PASSWORD BEHAVIOUR

In contrast to Section 7.1, which focused on the physical make-up of the passwords employed by the respondents, the focus of this section is on the security or otherwise of the respondents' passwords based on their behaviour in terms of password sharing. Questions 72, 73, 74, and 75 dealt with this subject, with the questions eliciting the respondents' actions relating to sharing their password, and their post-sharing actions.

7.2.1 PASSWORD SHARING

The initial question on this topic, Question 72 queried whether the respondents had shared their password, and if so with whom. These results are shown in Table 7.6.

***Table7.6**: Password sharing habits*

Shared with	Total (n=258)	%	Male (n=122)	%	Female (n=136)	%	p-value
Friend	157	60.85	71	58.20	86	63.24	0.413
Family member	137	53.10	59	48.36	78	57.35	0.149
Acquaintance	5	1.94	4	3.28	1	0.74	#
Boyfriend or girlfriend	28	10.85	17	13.93	11	8.09	0.137
Stranger	3	1.16	2	1.64	1	0.74	#
Password not shared	50	19.38	26	21.31	24	17.65	0.469
Involvement in any sharing	204	79.07	94	77.05	110	80.88	0.453

 # p-value not calculated due to small sample size

The figure that is immediately eye-catching in Table 7.6 is the high proportion (79.07%) of respondents overall, who had shared their password. This is reflected as *involvement in any sharing* in the last row of the Table, and was calculated by allocating a positive value to all respondents who had answered 'yes' to password sharing in any one of the provided categories. This result follows the established theme of lack of awareness of or disregard for the consequences of password compromise (whether by wilfully imparting knowledge of the password to someone else, or by unwitting comprise, such as via a phishing attack).

Interestingly, answers to Question 75 show that 59.30% of all respondents had used another person's password to access their computer or email, which is some 20% less than those who admitted to sharing their password(s). This could indicate that in some cases passwords were shared, and then not used, the reasons for which, if it were indeed the case, would warrant a separate investigation. The figure could also indicate that other people's passwords were used to access accounts other than computer logons and email, for example social media or other accounts, an option which was not explored in the questionnaire.

The majority of respondents shared their passwords with friends, with the next most significant group with whom sharing took place being family. While these two groups, especially the latter may carry a lower risk of account abuse, information theft, or privacy breaches via the shared password than the other categories owing to the real or perceived trust based nature of these relationships, the potential still exists. Particularly in the case of friends, the password may be shared with others and private data accessed without consent (for example resulting in the distribution of material relating to sexting or the contents of private messages being read). While the risk of family members redistributing the password or the contents of messages or photographs, it is perhaps unlikely that the respondents to this survey, given their age, would have wanted family members to have full access to their private information.

The next most common group with whom sharing took place was with a boyfriend or girlfriend. As with sexting this poses a high risk, for relationships can end, and at that point the private data of the partner who had shared any of their passwords would be

accessible to a potentially spiteful former partner. More encouragingly from a risk point of view, are the low numbers of respondents who had shared passwords with strangers or acquaintances. Although low numerically, the respondents indicated that they were more willing to share explicit photographs or videos of themselves with strangers and acquaintances than they were their passwords. This is positive from a password security perspective, but not from a personal information security or online privacy perspective.

Considering the high number of respondents who admitted to sharing their passwords, the answers provided to Question 73 are interesting: 58.52% of the total number of respondents indicated that they had *not* changed their passwords after sharing them. This included respondents who had answered as 'non applicable', implying that they had not shared their passwords. When an analysis was carried out of respondents who had actually both taken part in some form of sharing (as reflected in Table 7.6) , *and* who had changed their passwords after sharing them according to Question 73, the result was only 21.7%. This figure is consistent with the other results obtained in this section, revealing the lack of awareness and/or concern about the negative possibilities associated with someone else having access to any of one's passwords.

Perhaps of more concern is that an analysis of respondents who used the same password for more than one account *and* who had changed their password after sharing revealed that only 11.24% of the total number of respondents had done so. When refined further, those who had used the same password for more than one account *and* who had shared *and* who had changed their password after sharing totalled only 26 respondents, or 10.07%. In contrast, those who met the first two criteria but who had not changed their password after sharing totalled 97 respondents, or 37.59%, a marked difference.

In gender terms, there is no statistical evidence to suggest that male and female respondents differed in terms of likelihood or actual practice of password sharing. Additionally when broken down by category of answer, there is no evidence that male respondents were more or less likely to share within any of the categories than female respondents.

Having established the incidence rate of password sharing amongst the respondents, the next step was to determine the reasons for the respondents exhibiting this behaviour. This was addressed in Question 74, which required the respondents to provide an explanation of their own choice of why they had shared a password. The answers received ranged from the incomprehensible to the realistic, and many were not particularly explanatory. The common theme among those who provided actual reasons was that passwords had been shared to enable friends to access the computer (or telephone) for various reasons while the owner of the items was not present. Why this was necessary was not elaborated upon in all cases, but the general trend appeared to be so that the other party could either make use of the computer operationally, or access work/media on the computer in the absence of the owner. This is congruent with the low rate of post sharing password change, as continued access via the shared password was implied.

Of the other reasons provided for password sharing, 'trust' and 'because they asked for it' (the password) were also among the more common answers provided. There were also the occasional answers that stuck out but which were only provided by a single or small numbers of respondents. These included sharing the password for money or that their parents wanting to check their emails. What can be inferred from these answers, and the ones above, is that little or no concern for privacy was exhibited by the respondents in terms of allowing access to their computers, telephones, files, and messages.

7.3 SUMMARY

Considering the attitudes displayed towards password security as examined in Section 7.2, it was concluded that the respondents risk level in terms of passwords (both in terms of behaviour and construction), and therefore security and/or privacy breach was high. Taking into account the similar result of high risk in terms of password construction in Section 7.1, the overall risk level was classified as high, and thus in need of rectification. No significant gender differences were identified in this section, and as such the risk was spread between all respondents.

CHAPTER 8: CONCLUSIONS AND FUTURE WORK

8.1 CONCLUSIONS

The primary objective of the research was to produce data that could provide insight into the awareness of information security threats and online behaviour at senior secondary school level, within the broader context of information security. Data covering types of threats, the risks posed by these threats, online privacy, and cyberbullying was collected, analysed and discussed. Actual experiences and online behaviour were also investigated and assessed. Sub-objectives included the determination of any significance in gender differences, and the investigation of the relationship (if any) between perceived awareness and behaviour, as well as the differences between perceived and actual knowledge (awareness) based on both answers given to direct questions, and interpretation of online behaviour.

In overall terms of awareness, it was apparent that not only was the actual level of awareness low, as originally hypothesised, but there was a large gap between the level of knowledge possessed by the respondents, and the level which they perceived themselves to have. This held true across all of the areas analysed. More specifically, there were notable gaps in the conceptual knowledge, awareness and the practice of online privacy, and the existence and understanding of external online threats. The topic of sexting was addressed in some depth, and while the practice was not widespread, there was enough involvement to warrant concern regarding this behaviour, from a perspective of the personal ramifications to the learners involved. Analysis of behaviour and attitudes towards passwords also revealed behavioural deficiencies in security terms. The assessment of cyberbullying showed it to be a problem at an individual rather than institutional level, although it was not widespread.

Based on these results it can be concluded that as a group, the respondents were generally unaware of the threats to their online safety and security. Additionally, it was shown that significant levels of risky online behaviour were exhibited by the respondents, and that privacy was not considered to be an overriding concern. The respondents in this survey were shown to be at a generally high level of risk in terms of threats to their information security, online privacy, and indeed online *safety*, owing to

their lack of awareness and behaviour patterns. This risk level is indicative of the need for awareness education, through the form of structured awareness programmes. The results of the study indicate that education should focus not only on the concepts, but on awareness and behaviour in practice as well.

The investigation of gender differences based on the answers provided by the male and female respondents showed that there were instances of gender superiority in some areas. Male respondents were shown to have slightly higher overall awareness levels, but were however also shown to be more likely to exhibit high risk behaviour such as engagement with strangers, to show less concern, awareness and willingness to engage with the concept of online privacy, and to be more likely to engage in sexting, particularly in the practice of disseminating material to third parties. Conversely female respondents showed more awareness about the concept of privacy, were more willing to engage with related policies, and more likely to have taken steps to improve their online privacy. While these differences were apparent, neither gender showed either a complete lack of knowledge or a total knowledge of the subject area. It can thus be concluded that owing to both the overall low levels of awareness shown, and the gender differences exhibited, that gender should not influence the content of structured threat awareness programmes, although it may influence how the information is conveyed.

8.2 FUTURE WORK

Finally, there is much scope for future work in this area based on the conclusions above. As this is an area that has not been widely covered in South Africa, and taking into account the cosmopolitan nature of the respondents, being boarding school learners, the conclusions reached could have wider implications beyond the particular group of respondents sampled. Thus related future work could be carried out either based on, or allied to this research.

The material covered in each of the analysis and discussion chapters was carried out, provides opportunities for future research. There was a significant amount of data collected via the questionnaire that was not analysed due to the volume of data collected, while future research could also expand the depth of the material already covered as individual areas in this thesis. In particular the work done on the

relationship between privacy and social media, and the general awareness of terms could be expanded.

Further options for future work include the development of a model programme for addressing threat awareness at senior secondary school level. Research could also be done on the impact on the awareness and behaviour of learners who have been exposed to information regarding information security and awareness, such as those who have been part of this research process, compared to those who have not been, as they enter into university and beyond. As technology and its use evolve, and perhaps becomes more widespread in areas where not presently found, future studies could include historically disadvantaged schools, and focus more on cultural issues when developing or amending a more expansive model for threat awareness at secondary school level. Further, while it may be necessary to limit the scope of future research to awareness and behaviour related directly to information security, the potential exists for the scope to be extended to include a further focus on cyberbullying. This is an area that is directly related to threat awareness, and online behaviour and is linkable to the overall information security field. Future research could also delve into the effectiveness of an implemented awareness programme, which could be tested by post-implementation surveys and/or practical tests on whether the information provided has been well received.

Benefits to the schools would include a heightened awareness amongst learners and School Principals of the existence of online threats simply through exposure to the questionnaires and discussion. School leadership are provided with information regarding areas that could be regarded as problems, or vulnerabilities amongst their learners. These issues could be addressed during future research, and would form part of the developed threat awareness programme model mentioned above. Such a programme could be implemented in the future at schools to mitigate problem areas and vulnerabilities identified in this research. Independent of future research, the research findings could be used by schools to inform their own policies regarding awareness and education. This would meet the goal of providing early education to set learners on a path of security consciousness, which would be of benefit to them throughout their lives.

REFERENCES

Atherton, J. (2011). *Learning and Teaching: Bloom's taxonomy.* Retrieved December 2012 from http://www.learningandteaching.info/learning/bloomtax.html

Badenhorst, C. (2011). *Legal responses to cyber bullying and* sexting *in South Africa.* Retrieved December 2012 from http://www.cjcp.org.za/admin/uploads/Issue%20Paper%2010-1.pdf

Belsey, B. (2012). *Cyberbullying.org* Retrieved December 2012 from http://www.cyberbullying.org/

Bernard, A. (2005). *Crimeware on the Rise.* Retrieved December 2012 from

http://www.cioupdate.com/research/article.php/3530506/Crimeware-on-the-Rise.htm

Bowden , M. (2010). *The Enemy Within.* Retrieved December 2012 from http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/

Boyd, D., and Hargittai, E. (2010). Facebook privacy settings: Who care? *First Monday*, *15*(8), 2. Retrieved December 2012 from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Braynov, S. (2006). E-commerce vulnerabilities. In Bidgoli, H. (Ed). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management*. Volume 3, (pp 57-70).New Jersey, USA. Wiley Publishing.

Campbell, Q., and Kennedy, D. (2002). The Psychology of Computer Criminals. In Bosworth, S. and Kabay, M. (Eds). *Computer Security Handbook 4th Edition.* (pp 140-160). USA. Wiley and Sons.

Chan, T. (2006). *Spyware.* In Bidgoli, H. (Ed). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management.* Volume 3, (pp 136-143). New Jersey,USA. Wiley Publishing.

Cohen, L., Manion, L., and Morrison, K. (2011) Research Methods in Education. 7th Edition. London, UK. Routledge.

Debatin, B., Lovejoy, J., Horn, A., Hughes, B. (2009*).* Facebook and online privacy: Attitudes, behaviors, and unintended consequences*. Journal of Computer Mediated Communication*, 15(1), 83-108.

Dell'Amico, M., Michiardi, P.,Roudier, Y. (2010). Password strength: an empirical analysis.*. In Proceedings of INFOCOM (pp. 1-9).* San Diego, CA, USA. *IEEE.*

Dillman, D. A., Carley-Baxter, L., Jackson, A. (1999). Skip-pattern compliance in three test forms: a theoretical and empirical evaluation *#99-01. SESRC Technical Report.* Social & Economic Sciences Research Centre, Washington State University, USA.

Donath, J. (2010*). German schools to teach online privacy*. Retrieved December 2012 from http://www.spiegel.de/international/germany/0,1518,710320,00.html

Durheim, K., and Terre Blanch, M. (Eds). (1999). *Research in Practice* . Cape Town. South Africa. UCT Press

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems, 3(2), 112-126*.

Granger, S. (2002). *The Simplest Security: A Guide to Better Password Practices*. Retrieved December 2012 from : http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

Griffin, S. E., and Rackley, C. C. (2008,). Vishing. In *Proceedings of the 5th annual conference on* Information Security *Curriculum Development* (pp. 33-35). New York, NY, USA: ACM. DOI: 10.1145/1456625.1456635.

Hadnagy, C. (2010). *Social Engineering : The Art of Human Hacking.* Indianapolis, USA. Wiley Publishers.

Harley, D. (2006). Email threats and vulnerabilities. In Bidgoli, H. (Ed).). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management,* Volume 3. (pp 41-56).New Jersey, USA. Wiley Publishing.

Howard, F., and Komili, O. (2010). *Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware*. Technical Report, Sophos Labs. Retrieved December 2012 from http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/sophos-seo-insights.aspx

Ianella, R. (2006). *Digital Rights Management.* In Bidgoli, H. (Ed). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management*, Volume 3. (pp 865-787).New Jersey, USA. Wiley Publishing.

Jakobsson, M. , and Ramzan, Z. (2008). *Crimeware: understanding new attacks and defences*. Addison-Wesley Professional. Boston,USA.

Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34(3), 549*.

Keith, M., Shao, B., & Steinbart, P. (2009). A behavioural analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems, 10(2), 63-89.*

Li, Q. (2006). Cyberbullying in schools a research of gender differences. *School Psychology International* 27.(2): 157-170.

Lininger, R., and Vines, R. D. (2005). *Phishing: Cutting the Identity Theft Line.* Indianapolis , USA. Wiley.

Long, J. (2008).*No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* Burlington, MA, USA. Syngress.

Longman's Dictionary of Contemporary English. (2012). Retrieved December 2012 from http://www.ldoceonline.com/dictionary/419-scam

Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. In *Proc. of the 10th IEEE Intl. Conf. on Computer and Information Technology* (pp. 824-831).

Mann, I. (2008). *Hacking the Human*. Aldershot, UK. Gower Publishing Company, Limited.

Marwick, A., Murgia-Diaz, D., & Palfrey, J. (2010). *Youth, privacy and reputation (literature review).* Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10-29. Retrieved December 2012 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163

McCreevy, J. (2002) Footprinting. What is it, who should do it, and why ? *SANS White Paper*. Retrieved December 2012 from http://www.sans.org/reading_room/whitepapers/auditing/footprinting-it-it-why_62

Microsoft. (2009). *Strong Passwords*. Retrieved December 2012 from http://msdn.microsoft.com/en-us/library/ms161962.aspx

Microsoft. (2011). *Teen Online Reputation: 13 – 17 Years Old*. Retrieved December 2012 from http://www.microsoft.com/security/resources/research.aspx#teen

Mitnick, K., and Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, USA. Wiley Publishers.

Mitnick, K., and Simon, W. (2005). *The Art of Intrusion*. Indianapolis, USA. Wiley Publishers

Ollmann, G. (2007). The vishing guide. Retrieved December 2012 from http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf

Parker, A. (2002). *Toward a new framework for information security.* In Bosworth, S., and Kabay, M. (Eds). Computer Security Handbook 4th Edition. (pp 116-138). USA. Wiley and Sons.

Redline, C. D., Dillman, D. A., Carley-Baxter, L., & Creecy, R. (2003). Factors that influence reading and comprehension in self-administered questionnaires. In *Workshop on Item-Nonresponse and Data Quality,* Basel Switzerland. Retrieved December 2012 from http://survey.sesrc.wsu.edu/dillman/papers/2003/factorsthatinfluencereading.pdf

Republic of South Africa. (1996). *Films and Publications Act,65 of 1996.*Republic of South Africa. [Laws].Retrieved December 2012 from http://www.info.gov.za/view/DownloadFileAction?id=70901

Republic of South Africa. (2002). *Electronic Communications and Transactions Act 25.* Republic of South Africa. [Laws].Retrieved December 2012 from http://www.info.gov.za/view/DownloadFileAction?id=68060

Republic of South Africa. (2007). *Sexual Offences and Related Matters Amendment Act 32 of 2007*. Republic of South Africa. [Laws].Retrieved December 2012 from http://www.info.gov.za/view/DownloadFileAction?id=77866

Republic of South Africa. (2008). *Child Justice Act 75 of 2008*. Republic of South Africa. [Laws].Retrieved December 2012 from http://www.justice.gov.za/vg/cj/2010_NPF_ChildJustice_tabled21may.pdf

Republic of South Africa. (2009). *Films and Publications Amendment Act 3 of 2009*. Republic of South Africa. [Laws].Retrieved December 2012 from *http://www.info.gov.za/view/DownloadFileAction?id=106329*

Rice, E., Rhoades, H., Winetrobe, H., Sanchez, M., Montoya, J., Plant, A., & Kordic, T. (2012). Sexually Explicit Cell Phone Messaging Associated With Sexual Risk Among Adolescents. *Pediatrics,* 130(4), 667-673. DOI: 10.1542/peds.2012-0021.

Roper, C., Fischer, L., & Grau, J. A. (2005). Security Education, Awareness and Training: SEAT from Theory to Practice. Oxford, UK. Butterworth-Heinemann.

Siciliano, R. (2012). *Protect yourself from Phishing.* Retrieved December 2012 from http://blogs.mcafee.com/consumer/protect-yourself-from-smishing

Skinner, C. (2010*). 65% of Web Users Are Victims of CyberCrime*. Retrieved December 2012 from http://www.pcworld.com/article/205309/65_of_web_users_are_victims_of_cybercrime.html

Steeves, V. (2010). *Summary of Research on Online Youth Privacy*. Retrieved December 2012 from http://www.priv.gc.ca/information/pub/yp_201003_e.pdf

Sonhera, N., Kritzinger, E., & Loock, M. (2012). A proposed cyber threat incident handling framework for schools in South Africa. In *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference (pp. 374-383).* New York, NY, USA ACM.

The National Campaign. (2008). *Sex and Tech – Results from a survey of teens and young adults*. Report of the National Campaign to Prevent Teen and Unplanned Pregnancy, Washington, DC, USA. Retrieved December 2012 from http://www.thenationalcampaign.org/sextech/pdf/sextech_summary.pdf

The Open Web Application Security Project. (2012). *Guide to Authentication*. Retrieved December 2012 from https://www.owasp.org/index.php/Guide_to_Authentication

The Oxford Dictionary. (2012). Retrieved December 2012 from http://oxforddictionaries.com/definition/english/sexting?q=sexting

Tipton, H., and Krause, M. (2004). Information security *Management Handbook.* 5th Edition USA. CRC Press.

Unknown A. (2011). Cyberbullying Resource Centre. Retrieved December 2012 from http://www.athinline.org

Vacca, J. (2009). *The computer and Information Security Handbook*. Burlington, USA. Morgan Kaufmann.

Vacca, J. (2010). *Managing* Information security. Burlington, USA. Syngress.

Van Niekerk, J., & Von Solms, R. (2008). Bloom's taxonomy for information security education. Information security *South Africa (ISSA).* Johannesburg, South Africa: ISSA.

Willard, N. (2006). Cyberbullying and cyberthreats. *Eugene, OR: Centre for Safe and Responsible Internet Use)*. Retrieved December 2012 from http://mcoehr.marinschools.org/SafeSchools/Documents/BP-CyberBandT.pdf

Witte, J. C., Amoroso, L. M., and Howard, P. E. (2000). Research Methodology Method and Representation in Internet-Based Survey Tools: Mobility, Community, and Cultural Identity in Survey2000. *Social Science Computer Review*, *18*(2), 179-195.

Young, A. (2006). *Trojan horse programs.* In Bidgoli, H. (Ed). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management*. Volume 3, (pp 107-118).New Jersey, USA. Wiley Publishing.

APPENDIX A: SEXTING AND CYBERBULLYING CASES AND MEDIA REPORTS

A paper titled "Legal responses to cyber bullying and sexting in South Africa.", providing legal implications and case examples of these behaviours.

http://www.cjcp.org.za/admin/uploads/Issue%20Paper%2010-1.pdf

An example of the worst outcome of sexting and cyberbullying where this behaviour resulted in a teenage suicide:

http://studentservices.dadeschools.net/sexting/pdfs/Her_Teen_Committed_Suicide_Over_Sexting.pdf

Another example of the worst outcome of sexting and cyberbullying where this behaviour resulted in a teenage suicide, as referred to in Chapter 6:

http://www.vancouversun.com/technology/Vancouver+area+teen+commits+suicide+after+telling+story+being/7375941/story.html

Related material to the above, providing more insight into the murky online world of sexting and 'capping':

http://www.salon.com/2012/10/21/amanda_todds_only_the_start/

A media article related to dealing with cyberbullying:

http://www.news.com.au/technology/tony-abbott-slams-facebooks-hands-off-approach-to-cyber-bullying/story-e6frfro0-1226518125646

An example of cyberbullying and its effect:

http://www.smh.com.au/world/teenager-uses-pigtail-power-to-defeat-her-school-bullies-20121101-28lyg.html

APPENDIX B: THE QUESTIONNAIRE

Online Information Security Threat Awareness and Behaviour Questionnaire

The purposes of this questionnaire are to assess the awareness of online threats to information security, and to determine online behaviour patterns in school learners with access to the relevant technology in the Grade 10 to 12 bracket. This Survey will be active from midnight 13/05/2012.

There are 98 questions in this survey

Consent

[A]Are you aware that your School Head has given consent for this survey to take place, and do you understand that this is an anonymous survey?

Please choose **all** that apply:

- Yes

Section A: Demographics / Background

[1]What is your age?

Please write your answer here:

-

[2]What is your gender?

Please choose **only one** of the following:

- Male
- Female

[3]What School Grade are you in?

Please choose **only one** of the following:

- Grade 10
- Grade 11
- Grade 12

[4]Are you a boarder or a daypupil?

Please choose **only one** of the following:

- Boarder
- Daypupil

- Other

[5]Do you have a personal (not a lab or shared family) computer (desktop, laptop, or iPad for example) ?

Please choose **all** that apply:

- Yes
- No

[6]Do you have regular (at least 3 or more times a week) access to a computer (desktop, laptop, or iPad for example) at school?

Please choose **all** that apply:

- In a computer lab
- In your room
- Elsewhere:

[8]If at home, is your computer usage monitored in any fashion by your parents?

Please choose **only one** of the following:

- Yes
- No

[9]Do you own a cellphone?

Please choose **only one** of the following:

- Yes
- No

[12]Do you primarily access the internet via cell-phone or computer?

Please choose **all** that apply:

- Computer
- Cellphone
- Other:

[13]What make or model of cellphone do you have?

Please choose **all** that apply:

- Blackberry
- Nokia
- Samsung

- iPhone
- Other:

[14]Rate your general awareness of internet and software threats to Information Security, and online privacy issues:

Please choose **only one** of the following:

- I regard myself as very aware
- I am aware of some of the terms and issues
- I have head of some these, but not aware of what they mean
- I regard myself as quite unaware

[15]Do you estimate your weekly computer usage to be:

Please choose **only one** of the following:

- Daily
- 1-2 Days per week
- 2-3 Days per week
- More than 4 days per week but less than 7

[16]How many hours a day do you spend using your computer or cellphone to access online services (including the internet, text and instant messaging)?

Please choose **only one** of the following:

- 1 Hour or less
- 1-2 Hours
- 2-3 Hours
- More than 3 hours

Section B: Social Media

[17]Do you make use of any of the following Social Media applications or platforms? Mark all applicable:

Please choose **all** that apply:

- Facebook
- Myspace
- Whatsapp
- Blackberry Messenger

- Mxit
- Twitter
- Google+
- Bebo
- Youtube
- Gtalk
- MSN Messenger
- Pidgin
- Yahoo Messenger
- Ou Toilet
- AOL
- Skype
- Other:

[18] Which three of the Social Media application that you selected above do you use the most ?

Please write your answer here:

[19]Do you access these mostly via :

Please choose **all** that apply:

- Cellphone
- Computer
- One just as often as the other

[20]How often do you use Social Media platforms ?

Please choose **all** that apply:

- Daily
- 3-5 Days per week
- 2-3 Days per week
- Less than 2 Days per week

[21] How much of your total time on the internet do you spend on Social Media ?

Please choose **all** that apply:

- Most of my total time

- More than half my total time
- About half my total time
- Less than half my total time

[22] Why do you use Social Media Platforms ?

Please choose **all** that apply:

- To maintain connections with my friends and family
- To meet new people
- To discuss topics of interest with like-minded people
- To share photos
- Other:

[23] What in your opinion are negatives of the use of Social Media? Please list them below.

Please write your answer here:

[24] Do you prefer to communicate on your cellphone using :

Please choose **all** that apply:

- Text Messaging
- Instant Messaging (for example Whatspp or Gtalk)
- Voice
- Other:

[25] Have you ever sent a request to add a person you have not physically met to an online friend or contact list?

Please choose **only one** of the following:

- Yes
- No

[26] Was this person the same gender as you ?

Please choose **only one** of the following:

- Yes
- No
- Not Applicable

[27]Was this person within 5 years of your age ?

Please choose **all** that apply:

- Yes, younger
- Yes, older
- Not within 5 years of my age
- Not Applicable:

[28] Have you ever accepted an invitation (friend request) from a person you have not physically met to an online friend or contact list ?

Please choose **only one** of the following:

- Yes
- No

[29] Was this person within 5 years of your age ?

Please choose **all** that apply:

- Yes, younger
- Yes, older
- Not within 5 years of my age
- Not Applicable:

[30] Was this person the same gender as you ?

Please choose **only one** of the following:

- Yes
- No
- Not Applicable

[31] Have you ever received personal communication from a person you have not physically met ?

Please choose **only one** of the following:

- Yes
- No
- Not Applicable

[32] Have you ever engaged in online communication with a person you have not physically met ?

Please choose **only one** of the following:

- Yes
- No
- Not Applicable

[33] If so, has this happened:

Please choose **all** that apply:

- Once only
- Less than 3 times
- Up to 5 times
- More than 5 times
- Not Applicable

[34] If applicable, who initiated the contact ?

Please choose **only one** of the following:

- Me
- The other person
- Not Applicable

[35] Have you ever provided any personal information to someone you have not physically met, such as:

Please choose **all** that apply:

- The name of your school
- Your Location
- Any details of your family
- Any details of your friends
- Financial details
- Your phone number (Home, hostel, or cell)
- Your email address
- Not applicable
- Other:

Section C: Direct Awareness of Threats

[36] Have you encountered any of the following terms ? Mark all of the applicable ones

Please choose **all** that apply:

- Phishing
- Identity Theft
- Social Engineering

- Smishing
- Vishing
- Keystroke Logging
- Spam
- Computer Virus
- Online Privacy
- Cybercrime
- Crimeware
- Malware
- Spyware
- Trojan
- Computer Worm
- Spoofing
- Spam
- Browser Poisoning
- WSUS
- 419 Scam
- None of the above

[37] In terms of the Information Security Threats provided in the list below do you consider yourself:

Please choose **all** that apply:

- Very Aware : I am confident I know what is out there
- Aware : I am aware of threats as concept, but do not do much about it
- Less Aware : I have heard some of the terms, but do not know what they mean
- Unaware : This is all new to me

[38] Has your computer ever been infected by a virus ?

Please choose **only one** of the following:

- Yes
- No

[39] If so are you aware how it became infected ?

Please choose **all** that apply and provide a comment:

- Yes, and this is how (please describe)
- Yes I don't know how
- Not applicable

[40] Have you ever received unsolicited (not addressed to you personally or specifically) :

Please choose **all** that apply:

- Emails
- Instant Messages
- Text Messages (SMS)
- Not Applicable
- Other:

[41] Have you ever been asked for any personal information via

Please choose **all** that apply:

- Direct communication from a friend
- Direct communication from a stranger
- An unsolicted text message
- An unsolicited email
- Not applicable
- Other:

[42]If you have received unsolicited, impersonal communication, have you ever:

Please choose **all** that apply:

- Clicked on the attachment
- Clicked on the link provided
- Entered your username and password when requested
- Replied to the email or text message via text, email, or voice dialling
- Not Applicable

[43] If you have responded to or interacted with and unsolicited and impersonal message in any way, what was the outcome?

Please write your answer here:

[44] Are you aware that clicking on a harmful link can lead to a virus infection and / or theft of personal data?

Please choose **only one** of the following:

- Yes
- No

[45] Which of the following do you place online ?

Please choose **all** that apply:

- Pictures
- Videos
- Text and comments

[46] Have you ever placed anything online which you would not like your parents to see?

Please choose **only one** of the following:

- Yes
- No

[47] Do you have Anti-Virus Software on your personal computer if you have one?

Please choose **all** that apply:

- Yes
- No
- I do not have a personal computer

[48] Which Anti-Virus do you use on your personal computer ?

Please write your answer here:

[49] Do you run Automatic Updates on your personal computer ?

Please choose **all** that apply:

- Yes
- No
- I am not sure what those are

[50] Have you ever deliberately adjusted a the privacy or security settings on a web browser on any computer (home, personal, or school)?

Please choose **only one** of the following:

- Yes

- No

Section D : Behaviour and Privacy

[51] In the space provided please provide a brief description of your understanding of online privacy

Please write your answer here:

[52] Do you know how to use the privacy settings on your Social Networking Platform ?

Please choose **only one** of the following:

- Yes
- No

[53] Have you ever changed these settings?

Please choose **only one** of the following:

- Yes
- No

[54] Are you a member of a Network (for example 'Kingswood' / 'Rhodes' on Facebook or another Social Media site?

Please choose **all** that apply:

- Yes
- No
- I am not sure what a network is

[55] If you have ever left a network on a Social Media platform, please explain why

Please write your answer here:

[56] Have your ever taken any deliberate steps to improve your online privacy ?

Please choose **all** that apply and provide a comment:

- Yes (Please state what)
- No

[57] Have you ever thought that information or a photograph was private and later found it not be?

Please choose **only one** of the following:

- Yes
- No

[58] Do you list any of the following information about yourself on Facebook or other Social Media Platforms?

Please choose **all** that apply:

- Name Of Your School
- Date of Birth
- Age
- Cellphone number
- Relationship Status
- Blackberry Messaging PIN
- Home Telephone Number
- Boarding House Telephone Number
- Instant Messaging Contact Details
- Postal Address
- Home Address
- School Emaill Address
- Personal / Private Email Address
- Your Location
- Activities and Interests

[59]Please indicate which of the information on the left is visible on your Social Media Platform(s) to the options along the top.

[60] Are you aware of the privacy settings available to Facebook users?

Please choose **only one** of the following:

- Yes
- No
- I am vaguely aware

[61] Have you read the privacy policies on any of the Social Media platforms you used, such as Facebook and Google?

Please choose **all** that apply:

- Yes, and I understand the policies
- Yes, but I do not fully understand
- No I have not.

[62] Do you allow your cellphone to advertise your location when you go somewhere, via Facebook for example?

Please choose **only one** of the following:

- Yes
- Sometimes
- No
- I am not sure what this refers to

[63] Have you ever adjusted privacy settings on your phone?

Please choose **only one** of the following:

- Yes
- No

[64] How long is your computer logon password?

Please choose **only one** of the following:

- 5 Characters or less
- 5-10 Characters
- Longer than 10 Characters

[65]How often do you change your computer logon password?

Please choose **only one** of the following:

- Monthly or more
- Once or twice a year
- Yearly
- Never

[66] How many different passwords do you have ?

Please write your answer here:

[67] Do you use the same password for:

Please choose **only one** of the following:

- More than one account (i.e. computer logon and Instant Messaging logon) but not all of them
- All of your accounts
- I have separate passwords for each account.

[68]How many different accounts (for example computer logon, Skype, Facebook, gmail etc) do you have?

Please write your answer here:

[69] Are you familiar with the term passphrase?

Please choose **only one** of the following:

- Yes
- No

[70] Is your password constructed from any of the following? :

Please choose **all** that apply:

- A dictionary word
- A combination of two or more words
- A sentence (not separated by spaces)
- A combination of words, numbers or letters and other characters
- Numbers only

[71] Do you use any of the below for a password? :

Please choose **all** that apply:

- Your date of birth
- A significant other's (boyfriend or girlfriend) date of birth
- A family member's date of birth
- Your Name
- A significant other's (boyfriend or girlfriend) name
- Someone else's name
- A pet's name
- A telephone number
- The word 'password' , the numbers '1234' or a blank password
- None of the above

70 [72] Have you ever shared your password(s) with:

Please choose **all** that apply:

- A friend

- A family member
- An acquaintance
- A boyfriend or girlfriend
- A stranger
- I have never shared my password

[73] Did you change the password after sharing it?

Please choose **all** that apply:

- Yes
- No
- Not Applicable

[74] For what reason did you share the password?

Please write your answer here:

[75] Have you ever used another person's password to access their computer or email ?

Please choose **only one** of the following:

- Yes
- No

Section E: User Experience

[76] Are you familiar with the terms *sexting* ?

Please choose **only one** of the following:

- Yes
- No

[77]Describe what you understand by the term *sexting*

Please write your answer here:

[78]Have you ever taken part in *sexting?*

Please choose **only one** of the following:

- Yes
- No

[79] Are you familiar with the term cyberbullying?

Please choose **only one** of the following:

- Yes
- No

[80]Describe what you understand by the term *cyberbullying*

Please write your answer here:

[81] Have you ever experienced *cyberbullying ?*

Please choose **all** that apply:

- Yes I have been on the receiving end
- Yes I have been involved in doing the bullying
- I have been on both the bullying and receiving end
- Not applicable

[82] Have you ever removed (or 'unfriended') someone as a friend on a social media or instant messaging platform ?

Please choose **only one** of the following:

- Yes
- No

[83] Has this resulted in a negative reaction toward you when discovered ?

Please choose **only one** of the following:

- Yes
- No

[84] Have you ever been removed (or 'unfriended') by a person or group of people ?

Please choose **all** that apply:

- Yes, and this resulted in a negative reaction
- Yes , and nothing came of it
- No, not that I am aware of
- Not applicable

[85] Have you received abusive or unpleasant message:

Please choose **all** that apply:

- In public, such as on a Facebook Wall, or via Twitter?
- In private , such as via email, inbox or text message
- Not Applicable

[86] Have you ever sent someone else an abusive message?

Please choose **all** that apply:

- Via Text Message
- Via Instant Message
- Via Inbox message or email
- Via public message, such as a Facebook Wall Post, or Twitter
- Not Applicable
- Other:

[87] If you have experienced cyberbullying or unpleasantness online did you experience this from

Please choose **all** that apply:

- Your peers (classmates or people of a similar agegroup)
- One or more older pupils at school
- One or more older people you know outside of school
- A person you have never physically met
- Other:

[88] Was the perpetrator or perpetrators (s) the same gender as you ?

Please choose **all** that apply:

- Yes
- No
- Not Applicable

[89] Through what mechanism did the bullying take place :

Please choose **all** that apply:

- Text messages
- Instant Messages
- Facebook
- Other Social Media platforms
- Email
- Not Applicable
- Other:

[90] What form did the bullying take

Please choose **all** that apply:

- Being disrespected
- Being made fun of
- Being called names
- Being threatened
- Receiving persistent unwanted contact or attention
- Not Applicable
- Other:

[91] Have you ever sent an explicit video or photograph of yourself to someone else?

Please choose **only one** of the following:

- Yes
- No

[92] Did you do this :

Please choose **all** that apply:

- By request
- Without being requested
- More than once ?
- Because you felt pressurised to
- To an older person
- To a younger person
- Not Applicable
- Other:

[93] Was the person you sent it to :

Please choose **all** that apply:

- Your boyfriend
- Your girlfriend
- A friend
- An acquaintance

- Someone you had only met online and not in person
- Not Applicable
- Other:

[94] Was the explicit picture or video sent via :

Please choose **all** that apply:

- Text Message
- Email
- Instant Messaging Application
- A web-based Social Media Site
- Not Applicable
- Other:

[95] Have you sent an explicit video or photo of someone you know to someone else?

Please choose **all** that apply:

- Yes to a friend
- Yes to a boyfriend
- Yes to a girlfriend
- Yes to someone you had only met online and not in person
- Not Applicable
- Other:

[96]Was this done with the person's consent?

Please choose **only one** of the following:

- Yes
- No

[97] Have you ever received an explicit photo or video from:

Please choose **all** that apply:

- Your boyfriend
- Your girlfriend
- A friend
- An acquaintance

- Someone you had only met online and not in person
- Not Applicable
- Other:

[98] Was the explicit picture or video received via:

Please choose **all** that apply:

- Text Message
- Email
- Instant Messaging Application
- A web-based Social Media Site
- Not Applicable
- Other:

[99] Have you ever hear of South Africa's ECT Act?

Please choose **only one** of the following:

- Yes
- No

[100] Did you find taking part in this questionnaire has made you more aware of issues surrounding online Information Security and Privacy ?

Please choose **only one** of the following:

- Yes
- No